Year 2000 Readiness Kit

A Compilation of Y2K Resources for Schools, Colleges and Universities

November 1998

U.S. DEPARTMENT OF EDUCATION

Acknowledgements

The U. S. Department of Education would like to thank those institutions, organizations and individuals that have graciously contributed time and information for this Year 2000 Readiness Kit.

Among those we would like to specifically thank for their collaboration in developing, drafting and compiling this kit are the National Association of Student Financial Aid Administrators (NASFAA), the National Association of College and University Business Officers (NACUBO), the American Association of Collegiate Registrars and Admissions Officers (AACRAO), the National Association of Independent Colleges and Universities (NAICU), the Career College Association (CCA), and the American Association of Community Colleges (AACC).

Inside you will find examples of what several institutions have done and some of the tools they have developed to address the Y2K problem. We would like to thank them for allowing us to share their ideas with you. They include the University of Iowa, Boston College, Salish Kootenai College in Pablo, Montana, University of Notre Dame and Columbia University. We would also like to thank the New England Student Loan Marketing Association, United Educators Insurance Risk Retention Group, Inc., and the State of Minnesota Year 2000 Project in the Department of Administration for sharing their work.

We thank those institutions that completed surveys and attended focus groups where they shared with the Department and their member associations their own challenges and the lessons they learned as they addressed this issue. We would specifically like to thank Emory University, the University of California at Berkeley, the University of Southern Maine, NACUBO and NASFAA for hosting Y2K focus groups. Several members of the Federal Family Education Loan (FFEL) community have been very helpful in leading discussions on this subject as well. We would like to thank the National Council of Higher Education Loan Programs (NCHELP) and Student Loan Servicing Alliance (SLSA) for facilitating several sessions where invaluable feedback and information were shared among the Department, lenders, guaranty agencies and third-party servicers.

In addition, many people have taken a leadership role in raising awareness of the Y2K issue and providing technical assistance to others. We would like particularly to thank all those who have helped get the word out about our upcoming Year 2000 Teleconference and those institutions that are acting as community host sites.

This Year 2000 Readiness Kit is not intended to provide a complete solution to the Y2K problems at education institutions, but we hope you find the checklists, resources lists, tools and the examples of what others have done useful complements to your own Y2K project. In addition to the examples in this kit, there are many Y2K plans on the Web sites of other institutions; that would have been excellent additions to this readiness kit.

The U.S. Department of Education and the other institutions and organizations that provided information for this kit, make no representation as to the completeness or efficacy of any portion of this kit. The U.S. Department of Education and these other organizations make no warranties or representations about the information provided in this kit and have no responsibility for any results arising from its use.

This Year 2000 Readiness Kit and the Year 2000 Teleconference were produced by the U.S. Department of Education. They are in the public domain. The full text of this publication is available at the Department's home page at **http://www.ed.gov/y2k**, and in alternate formats upon request. Use, duplication and distribution are free and unrestricted. For more information, please contact us at:

U.S. Department of Education
Office of Postsecondary Education
Room 4082, ROB-3
Washington, D.C. 20202-5100
E-mail: ope_y2k@ed.gov
Telephone: (202) 708-5547 or 1-800-USA-Learn
FIRS 1-800-877-8339, 8 a.m. - 8 p.m., ET, M-F

Contents

SECTION

Introduction 1

1 **Year 2000 Information and Readiness Disclosure Act** 2
Statement by the President

2 **Description of the Y2K Problem**

Description of the Y2K Problem 3

Y2K Readiness Assessment of Postsecondary Institutions 4

3 **Y2K Checklist for Institutions** 5

4 **Y2K Communications Strategy** 6

5 **Addressing the Problem**
Getting to the Heart of the Y2K Problem 7
—in Academic Departments, by Kerry A. Kearney

Watchlist of Key Dates 9

Embedded Processes, University of Notre Dame Year 2000 Web Site 11

6 **Sample Y2K Project Plans from Colleges**

- Boston College Year 2000 12
- Salish Kootenai College, Pablo, Montana 16
- University of Iowa Toolkit 2000 20

7 **Personal Computer (PC) Testing Instructions** 31

8 **Compliance of Vendors**
Managing the Y2K Compliance of 32
Suppliers and Business Partners, by Andrew Butz

Vendor Evaluation - Sample Letter to Vendors (Columbia University) 34

Guide to Evaluation of Vendor Compliance Claims (Columbia University) 35

Contract and Procurement Language 36

9 **Contingency Planning**
Contingency Planning Can Lessen the Impact 37
of Inevitable Y2K Failures, by B.L. Bruner

Contingency Planning Best Practice (State of Minnesota) 38

Contingency Planning Template (State of Minnesota) 42

*S*ample University Y2K Contingency Planning Process Project 43

10 **Y2K Information and Resources**

Y2K Internet Resources - Web Sites 44

Y2K Information from the U.S. Department of Education 45

Frequently Asked Questions (FAQs) Department of Education Y2K Web Site 46

Introduction

The U.S. Department of Education facilitated the development of this *Year 2000 Readiness Kit* to assist our partners in the postsecondary community. We have three purposes in distributing the Kit to you:

- We want to respond to requests we had from many of you and your colleagues to bring together in one place as many approaches and techniques as possible for responding to the Year 2000 challenge;
- We want to disseminate to the widest possible audience the feedback we have received from our partners as we convened Year 2000 focus groups across the nation over the past five months. Some of the documents and articles you will find in the Kit were given to us at the focus groups with a request that we continue to share them with others; and
- We want to ensure continuation of our cooperative relationship with you that has worked so often in the past when we have encountered common problems.

The Kit compiles a series of articles and management plans from organizations and education institutions of many types and sizes. We have kept it short so as not to overwhelm you with paper. However, to ensure that you can locate more detailed technical information as you need it, we have included an extensive list of Web sites and other resources that are available to you.

The information in the Kit should be useful to institutions at widely different stages of preparation:

- It includes articles that describe solid management approaches for organizing to confront the Year 2000 challenge for those institutions that may have just begun their Year 2000 initiative.
- Other articles discuss the Year 2000 problem as an "enterprise" concern that must be examined in every facet of your institution and its educational and business activities.
- The Kit contains information and approaches for dealing with the vendors who provide your institution hardware and software.
- Very significantly, we have included several resources for those of you who have begun contingency planning initiatives.

Contingency planning is an issue that became more and more prominent in our meetings with your colleagues this summer and fall. Leaders at postsecondary institutions are asking how they can continue to carry on their core educational functions in the event that campus systems or partner systems fail for a period of time. While contingency planning is a difficult task, we encourage you to read the information here about contingency planning and share it with your institution's Year 2000 Team.

Please also share the Kit with your campus colleagues and those at other institutions. We have deliberately printed it on one side and in black and white to make duplication as easy as possible, and we will add it to our Year 2000 Web site.

The Kit represents the culmination of a series of exchanges and dialogues with you that we believe were helpful to all of us. It provides you with information about the thoughtful and carefully planned responses to the Year 2000 issue from financial aid administrators, information technology specialists at your institutions, deans and presidents, managers in guaranty agencies and at lenders and servicers, and the professional associations that represent each of these constituencies.

As the Department's outreach efforts continue through the rest of this year and into 1999, we will continue to listen to your concerns and seek your guidance about effective ways we can work together to resolve Year 2000 concerns.

Section 1

Year 2000 Information and Readiness Disclosure Act

Due to the frequency of the exchange of data through electronic systems, awareness of the Y2K status of data trading partners is extremely important. To reduce the threat of liability faced by those who share information, Congress passed, and President Clinton signed, the Year 2000 Information and Readiness Disclosure Act. Following, find the statement by the president at the signing of the bill into law. The full text of the law can be found at: **www.y2k.gov/new/y2kact.html.**

Year 2000 Information and Readiness Disclosure Act

THE WHITE HOUSE
Office of the Press Secretary
For Immediate Release October 19, 1998

STATEMENT BY THE PRESIDENT

Today I am pleased to sign into law S. 2392, the "Year 2000 Information and Readiness Disclosure Act."

As our Nation prepares for the year 2000 (Y2K), we face an urgent need to address the Y2K problem, which may cause computers and embedded systems that run America's critical infra-structure to malfunction or even shut down. With little over a year until January 1, 2000, this is a serious global challenge that businesses and governments around the world must address.

Today, my Council on Year 2000 Conversion is launching "National Y2K Action Week," to urge small- and medium-sized businesses to take the necessary steps to ensure that the technologies they and their business partners depend upon are ready for the year 2000. Over the next 5 days, the Small Business Administration, the Department of Commerce, and several other Federal agencies will host Y2K educational events at their field offices across the Nation. As part of this week, we are also urging State, local, tribal governments, and community organizations to address this critical problem. More than 160 national organizations representing industries, professions, government, and the nonprofit sector have joined the Council in promoting Y2K action during this week.

This legislation will help provide businesses, governments, and other organizations with the necessary informational tools to overcome the Y2K computer problem. This Act, which builds upon a proposal my Administration submitted to the Congress in July, is an important bipartisan accomplishment. I particularly want to thank those in the Congress whose hard work and support of this legislation made its passage possible. Representatives Horn, Kucinich, Morella, Barcia, Leach, LaFalce, Hyde, Conyers, Dreier, and Eschoo and Senators Bennett, Dodd, Hatch, Leahy, and Kyl were integral to getting this work done and done quickly.

Many organizations have been reluctant to share valuable information about their experiences in dealing with the Y2K problem or the status of their Y2K efforts for fear of lawsuits. The Act's limited liability protections will promote and encourage greater information sharing about both experiences and solutions, which will significantly enhance public and private sector efforts to prepare the Nation's computer systems for the new millennium. However, the bill will not affect liability that may arise from Y2K failures of systems or devices.

While I understand that companies have a wide range of concerns related to the Y2K transition and potential litigation, we must also protect the rights of consumers. Therefore, this legislation is focused exclusively on exposure related to information exchange and would not cover statements to individual consumers in marketing a product normally used for personal use.

Firms within an industry confront similar challenges as they work to ensure that their computer systems are Y2K compliant. Although the Department of Justice has already indicated that competitors in an industry who merely share information on Y2K solutions would not be in violation of the antitrust laws, this Act creates a specific exemption from the antitrust laws for these activities. The limited antitrust exemption created by S. 2392 will make it easier for firms to cooperate with one another to solve the Y2K problem while continuing to protect consumers from industry agreements to boycott, allocate a market, or fix prices or output.

Information sharing will be important not only to those who have already made progress addressing the Y2K problem, but also to the many small business and State, local, and tribal governments that are just beginning their Y2K work. I urge trade associations and umbrella organizations to collect such information from their members and provide it to others through websites and other means devoted to discussing Y2K experiences and solutions. My Council on Year 2000 Conversion looks forward to working with Federal agencies, other levels of government, and consumer and industry groups in expanding the website, www.y2k.gov, that already supports activities related to our Nation's efforts to address issues related to the Y2K transition.

The Y2K problem is an enormous challenge, and we must meet it. Enactment of this legislation is a significant achievement toward allowing all of us to take a successful step into the new millennium.

WILLIAM J. CLINTON
THE WHITE HOUSE
October 19, 1998

Section 2

Description of the Y2K Problem

The following document succinctly describes the three main issues associated with the Y2K problem:

- Two-Digit Date Storage
- Leap Year Calculations
- Special Meaning for Dates

Description of the Y2K Problem

The Year 2000 (Y2K) problem stems from the early years of computer programming when every key stroke was critical. To save time and space, early computer programmers identified years with only the last two digits — assuming 19 as the first two digits (e.g. 1967 = 67). As the year 2000 approaches, these computers and programs will see the year as 00 or 1900, which is the root of the problem. The Y2K issue is not terribly difficult to understand from the technical point of view. It is the scope of affected systems and business processes that makes it challenging.

The problem can be sorted into three main issues: two-digit date storage, leap year calculations, and special meanings for dates. The implications of these three issues need to be addressed by all organizations. Unfortunately, there will be no simple fix to the year 2000 issue, no "silver bullet," due to the fact that the use of dates for calculations is pervasive throughout software and that usage is not standardized.

Two-digit date storage

The most common and most damaging problem occurs when software has been written to store and/or manipulate dates using only two digits for the year. Calculations built upon these dates will not execute properly because they will not see dates in the 21st century as being larger numbers than those in the 20th century. Example: 2000 - 1998 = 2 but 00 - 98 = -98. The result of this might be that your accounting software sees all accounts receivable as overdue due to the fact that no customers have paid in 98 years.

The two-digit date convention assumes that the century is "19." This assumption was regarded as a necessity in the early days of commercial computing because of the high cost of computer storage and memory.

Leap year calculations

Leap years are calculated by a simple set of rules. Unfortunately, there are systems and applications that do not recognize the year 2000 as a leap year. This will cause all dates following February 29, 2000 to be offset incorrectly by one day. The rules for leap year calculations are as follows. A year is a leap year if it is divisible by four, but if it is divisible by 100 it is NOT a leap year, but if it is divisible by 400 it IS a leap year. Thus, the Year 2000 is a special case leap year that happens once every 400 years.

Special meanings for dates

The third main Year 2000 component is more commonly found in older computer programming. In order to write more efficient programs that allowed for the use of less memory, date fields were sometimes used to provide special functions. The most common date used for this was 9/9/99. In some applications the use of the special date meant "save this data item forever" or "remove this data item automatically after 30 days," or "sort this data item to the top of the report." Within each organization, special date codes may have been used differently. This is one of the main reasons that no single tool can locate all uses and/or misuses of date data.

Technically, the problem is simple to understand. The solutions to the problem tend to be fairly simple as well. The scope of the problem, however, makes it difficult. Every piece of hardware, software, and embedded system must be taken into account. Everything from mission-critical central accounting systems to small convenience applications must be examined for date-handling and how those dates might affect the rest of the environment.

Y2K Readiness Assessment of Postsecondary Institutions

Summary of Year 2000 readiness surveys performed by the Department of Education and the American Association of Community Colleges

According to Year 2000 readiness surveys conducted during the summer of 1998 by the Department of Education of Direct Loan schools, and by the American Association of Community Colleges, the percentage of postsecondary institutions that have not yet achieved Year 2000 compliance ranges from 63 percent to 81 percent depending on the category of school. Approximately one third of the schools that responded reported that a written Y2K plan does not exist at their campus. While approximately 83 percent reported some obstacle in achieving Y2K readiness, 60 percent to 90 percent, depending on school type, reported to be very confident in their ability to achieve Y2K compliance by March 1999. Frequently reported obstacles include: shortage of experienced personnel, funding shortages, lack of cooperation from vendors, competing priorities, project scope, inadequate project management structure, and lack of senior management involvement.

The Department of Education has a joint project with the Council of Great City Schools to survey the state of Y2K readiness in the nation's 50 largest school districts. In an initial survey conducted during the spring of 1998, the data indicate that the level of readiness was very uneven. A follow up survey was launched in the fall of 1998. In addition, the Department provided Quality Education Data with Year 2000-related questions for its fall survey of school districts in 20 states. The results of these surveys will be available in late 1998.

Most experts consider the existence of a Year 2000 project plan as one indicator of the likelihood of achieving year 2000 readiness. Therefore, due to limited time remaining, the large number of schools not yet compliant and that report not having a plan, as well as the high number that report obstacles, there is cause for concern. Three sample plans can be found within this Kit and many more can be found on the internet at: **www.educause.edu/issues/y2k.html.**

Section 3

Y2K Checklist for Institutions

The following checklist can serve to help a manager and staff logically think through the Y2K project management process and to facilitate the development of an expanded and individualized plan.
It can also be used to gauge the thoroughness of the current plan. It identifies *some* of the key steps and components that should be considered when addressing the Y2K problem.

Y2K Checklist for Institutions

Note: This checklist is designed to help you get started with planning for Y2K. It is not designed to be a comprehensive list of every task that needs to be completed in order for your institution to be ready for Y2K.

____ Form a Y2K task force or working group; identify team members and a member of senior management as chair.

____ Prepare a budget and allocate funds for the Y2K effort.

____ Prepare an inventory of all business processes, systems, personal computers, and equipment with embedded chips (see document entitled "Embedded processes") in use at your institution. Be sure to include systems supporting:

- ____ Student information/registrar
- ____ Admissions
- ____ Business office
- ____ Financial Aid office
- ____ Academic departments
- ____ Libraries
- ____ Human resources
- ____ Payroll
- ____ Accounting systems
- ____ Facilities, buildings, and grounds
- ____ Alumni affairs
- ____ Development
- ____ Campus fire, police, and security
- ____ Telecommunications systems
- ____ Research facilities
- ____ Hospitals, infirmaries, EMS
- ____ Medical school
- ____ Student computers
- ____ Auxiliary services: mail, food services, day care, stores, conference centers, hotels.

_____ Review all vendors and 3rd party trading partners that provide goods, services, or information to the institution and assess risks associated with Y2K failure by any of them. Obtain Y2K compliance reports from all vendors.

____ Test each system for compliance.
Include in the testing:

- Hardware
- Operating systems
- Custom code
- Applications (software)
- Data interfaces

____ Prioritize system upgrades and fixes that need to be made.

- Identify critical data processing systems. Fix those first, acquire a replacement system, or develop a work-around solution.
- Systems whose loss would disrupt operations.
- Systems whose loss would create a minor inconvenience.
- Systems that are extraneous (may be replaced).

____ Fix or replace hardware.

____ Fix or replace software.

- Fix the code if you can.
- Acquire new software if necessary.
- Outsource the process to a third party servicer if necessary.

____ Fix or replace embedded systems and interfaces.

- Embedded: elevators, water, security, heating and cooling systems, etc.
- Interfaces with all outside vendors and business partners.

____ Test all remediated and replaced systems well in advance of 1/1/2000.

____ Monitor the changes and fixes as they are accomplished.

____ Prepare necessary operational changes in your office. Develop and implement revamped backup procedures to ensure minimal loss of data because of the Y2K problem.

____ Make contingency plans for all systems, equipment, vendors, processes, and data. Include temporary outsourcing as one alternative.

____ Arrange for alternative sources of credit should a delay in receivables occur due to Y2K problems with third parties.

____ Document every step you take in your Y2K compliance efforts.

Section 4

Y2K Communications Strategy

Sharing Y2K information is vital to successfully fixing the problem as well as for addressing the anxiety resulting from a lack of information. In the following document, you will find:

- Reasons a Postsecondary Institution needs a Y2K Communications Strategy
- Elements of a Y2K Communications Strategy
- Constituencies Impacted
- Important Components of Periodic Y2K Reports

Y2K Communications Strategy

Why does a postsecondary institution need a Y2K Communications Strategy?

- Students, parents, faculty and staff, alumni and governing boards deserve complete and accurate information about the vulnerability of processes and facilities that are dependent on computers. These groups could begin asking questions at any time.
- External reporting—to governing boards, state officials, etc.—helps raise internal awareness and helps keep the institution's systems renovation efforts on track.
- If serious Y2K failures DO occur (despite everyone's best efforts), communications with students, faculty, and staff will become even more critical—to identify alternative procedures (contingency plans) and to report on progress in restoring normal systems.
- The news media will increasingly bring this issue to public attention—especially as we enter the year 1999.

Elements of a Y2K Communications Strategy:

(1) **Designate a Y2K communications office or officer** (e.g., public affairs office), to be responsible for answering all inquiries concerning the Y2K status of an institution's computer systems and business processes. This office should have an inventory of all data systems, and should receive up-to-date Y2K reports from all appropriate offices on campus.

(2) **Produce a series of clear Y2K status reports** (either special letters or special portions of normally occurring reports/ newsletters) concerning the institution's Y2K readiness efforts.

Constituencies that should get regular reports:

- Students (current and prospective) and their parents,
- Faculty and staff,
- Governing boards and owners of proprietary institutions,
- State officials and legislators (public nonprofit institutions),
- Alumni,
- Local press and radio/TV stations.

Periodic Y2K reports to constituencies should include:

- Information on the nature of the Y2K computer problem, and the extent to which the institution is dependent on computer systems.
- Summary of all relevant processes and services (e.g., payroll, finances, registrar, student accounts, student aid, admissions, health and other student services, teaching, administrative and research computer systems/networks/facilities, building security/power/water.)
- Current Y2K status of all relevant data systems (e.g., replaced by fully compliant new system, renovated and tested).
- The independent auditing firm (if any) which has been employed to test and verify the Y2K readiness of key data systems.
- Contingency plans designed to handle basic processes and services in the event of any Y2K-related data systems failures.
- Identification of the institution's Y2K information center/ officer, that can answer, or obtain answers to, all Y2K-related questions.

Section 5

Addressing the Problem

Understanding that there is a possible widespread Y2K problem is just the beginning. Focusing limited resources at a school on specific targets lays a foundation to identify and minimize risks to system functions. This section helps put the Y2K problem into an institutional setting:

- *Getting to the Heart of the Y2K Problem—in Academic Departments* describes specific steps that need to be taken to get different parts of a school to work together to solve Y2K problems
- Watchlist of key dates identifies certain dates that may cause problems to school systems during the coming months, and explains why those problems might arise.
- Embedded Processes provides a checklist of questions that will help identify products or systems at a school that pose Y2K risks due to their embedded technology or programming.

Getting to the Heart of the Y2K Problem—in Academic Departments

by Kerry A. Kearney

The computing environment at colleges and universities—marked by notoriously independent departments and even more fiercely autonomous faculty—makes solving the Year 2000 problem even more complicated than it is in other kinds of organizations.

At virtually every school, faculty members each have a computer (or several) and a network link, Software may come from the institution, and also from users, former users, and even students both present and long gone. Faculty members have probably learned to work quite easily in this chaotic state of affairs without the benefit of any kind of documentation whatsoever. Every university laboratory operates its own set of computers, stand-alone and networked PCs, Internet links, and communication ports. Various scientific devices and safety monitors rely on embedded computer chips to function.

There are other complications. Professors are almost universally computer literate, and many don't hesitate to substantially modify their hardware and software. However, they may not have documented those modifications, making it difficult to identify potential trouble spots. In addition, most colleges and universities rely on custom software applications to do everything from administering grants to managing laboratory processes. But faculty and staff may have retained little or no information on why or how these programs were coded as they were.

On top of it all, administrators may know little about who is using any of these computer resources. They may be even less aware of how the various pieces of the computer puzzle fit together.

Defining the Problem...

Even so, these hybrid systems probably serve as the central nervous systems of an institution's departments and labs, and they may work very well indeed—today. But they will not all work well throughout 1999 and into 2000 unless the institution undertakes a concerted effort to make the pastiche of computers, software, and embedded chip devices Year 2000 compliant. The risks of not doing so are high. Unless Y2K problems are fixed, calculations and date-related math may be wrong, erroneous data may be transmitted or mingled with good data, critical devices could cease to operate, and safety systems might no longer function.

Against this patchwork backdrop, administrators have no choice but to take charge of solving departmental Y2K problems. The administration must assume central responsibility for getting the work done; it cannot rely solely on individual departments or professors. These steps can help bring order to a process that at times may seem destined to spin out of control.

...and the Solution

The effort to bring each department into Y2K compliance is essentially a microcosm of the institution's broader effort. As such, departmental efforts will mirror the larger strategy and include similar elements.

The United Educators publication *The Year 2000 Challenge for Higher Education* details specific steps in this compliance process and suggests ways in which specific departments might be affected by Y2K problems.

Each department will have to inventory all its software, computers, devices, and communication equipment. Each item on the inventory will have to be assessed to determine if it needs to be brought into compliance. Then fixes need to be made where necessary, and those fixes need to be tested and then tested some more. Finally, each department needs to develop contingency plans in case unforeseen Y2K problems disrupt operations despite all the work.

Bridges Between Administration and Academic Departments

Even though all of the above will happen at the departmental level, it is important for the administration to drive the process.

The process will be easier and more effective if the institution's Year 2000 Task Force, charged with addressing Y2K issues across the board, includes someone who is specifically charged with coordinating activities within each department. Ideally, task force departmental liaisons will be faculty members. In some large institutions, the task force might include a representative from each department. In others, task force members may have liaison responsibilities with several departments. In either case, task force members must have enough clout and seniority to prevail on even the most senior tenured faculty members to cooperate with the effort.

Task force members must translate the institution's overall goals at the department level, developing and implementing a departmental plan and instilling a sense of urgency and commitment to solving Y2K problems. Diplomacy and tenacity may be required.

That diplomacy and tenacity will be tested as task force members work with departments to make the hard choices that Y2K compliance efforts require. Those choices fall into three categories, any one of which could spark resistance within the department:

Setting priorities. Task force members must help the department decide which processes to address. The department needs to determine which computerized functions are critical to achieving its mission and then it must rank

them in order of importance. Task force liaisons may be called on to moderate the spirited debate that can accompany the setting of department priorities.

Creating a schedule. The list of mission-critical priorities becomes the basis of the department's Y2K compliance schedule. There will not be enough time to fix every identified Y2K problem. Task force members can help the department first focus on equipment and processes that are mission critical. After those are taken care of, other problems can be addressed.

Establishing a budget. It will take money to solve Y2K problems, and, like time, there will not be enough of it. The budget probably will not support purchasing all new equipment, so the department will have to choose what to fix and what not to fix. Mediating this process will require task force members to have thick skins, and they will need to wield all the clout they can. Task force members can help departments work with the administration to find creative funding sources such as grants and targeted fundraisers.

Keep in mind that testing Y2K fixes can reasonably consume fully 60 percent of the Y2K schedule and budget. In a perfect world, each department might spend a year testing the fixes. That may be unrealistic, but the task force must ensure that everyone allows sufficient money and time for testing.

Despite close cooperation between the task force and departments, some Y2K problems are certain to crop up. Departments may experience unexpected errors and system failures. As the 1999 fall semester comes to a close, task force liaisons can encourage departments to back up files, print out critical documents, and otherwise prepare for the uncertain future of the new year.

The unique independence of college and university departments may make the Y2K problem difficult to solve, but it can be done. The administration must commit to fixing the problem at the departmental level, because departments are vital to institutional success. They provide the interface between faculty and students. They do the research that allows the school to apply for government grants. They publish the articles that provide prestige. The administration needs to convince its departments that Year 2000 problems must be fixed at the department level and then help them to do so.

Kerry Kearney is a partner in the Pittsburgh office of Reed Smith Shaw & McClay, UE's Select Counsel for that region. She is also co-chair of Reed Smith's Year 2000 Practice Group.
Reprinted with permission of United Educators Insurance Risk Retention Group, Inc., Education's Own Insurance Company, and UIMC, a management company serving education, copyright UIMC. "Risk & Reason" Fall 1998, Volume 6, Number 2. All rights reserved.

Watchlist of Key Dates

00/00/0000

This nonexistent date is sometimes used to trigger special logic. It may be used in a remediation to replace an actual date used as a special logic flag. This will usually not be an issue unless modifications to parsing login are necessary to allow its use.

1/1/1900 (Monday)

The number of days in a century is not evenly divisible by seven so no two consecutive centuries start on the same day of the week. If an algorithm disregards century information when making day of the week conversions, incorrect results may occur. (see also 1-1-2000).

12/31/1998

May cause rollover or reboot problems on some hardware.

1/1/1999

The first date having '99' as a two-digit year field. In many systems the date is parsed into individual year, month and day variables and the validity of the date is checked. Often an indicator is needed to trigger logic that reacts to a special situation. If the system ensures that the variable is a valid date, a specific year value or date may be used to indicate the special situation. The year '99' and dates within 1999 have been used for this purpose. When the reserved date occurs in normal data, the system may trigger special condition logic that doesn't apply to the situation.

4/9/1999

Special-use Julian date (99th day of 99th year)

7/1/1999

Many governments begin their 1999-2000 fiscal year.

8/21/1999

Global Positioning System date rollover affects military, transportation, Geographic Information System, and Vehicle Locator.

9/1/1999

Leading time horizon if 90-day billing is generated. The date 99-9 is commonly used to indicate an unknown date in a four-character data entry field that is only precise to the month. The input is interpreted to the full date 99-9-1 and stored. As long as the date is outside the range of normal data, it is recognizable as "placeholder" data. When the date 99-9 becomes a plausible entry for the field, it becomes difficult to tell which 99-9 is a real date and which is a placeholder that needs to be replaced with real data.

9/9/1999

This date is commonly used to indicate an unknown date in six-character (i.e., 99-9-9) data entry fields that do not require a leading zero. It was chosen because it was easy to type and yet far enough in the future to be easily differentiated from "real" dates. As 9-9-99 nears, it will become impossible for the computer user to know if the entry is valid or not.

9/10/1999

In systems that have used 9/9/99 as a never expire date, logic that allows deletion of data after a specified date may fail to protect data that should be restricted forever.

10/1/1999

Federal government and others begin FY 00.

12/31/1999

The last day that can be represented in standard six-digit date format without Y2K rollover risk. Since this date is sometimes used to trigger special logic, it must be established that the system is able to distinguish between a regular end-of year 1999 date and a special meaning date. For example, a license key intended to expire on 12-31-99 should not be confused with one that has no expiration date. This is also the start date for most Y2K rollover testing.

1/1/2000

The first day of the year 2000. A system with a day-of-week function based on six-digit dates may change from Friday, 1999-12-31 to Satuday, 2000-1-1 at Y2K rollover. There is a possibility that the date will be misinterpreted as 1900-01-01.

1/3/2000

First business day of the new year.

1/10/2000

This is the first seven-digit date after rollover if leading zeros are not used for day and month representations. Parsing functions may fail when the number of digits representing the day changes.

1/31/2000

First month-end.

2/28/2000

Day prior to leap year (to be used in rollover scenarios).

2/29/2000

The year 2000 is a leap year. Program logic used to identify leap years may be incomplete. This would cause date-processing errors for the remainder of the year. The Gregorian calendar provides an algorithm for leap year. If the system recognizes that a year evenly divisible by 100 is not a leap year and fails to recognize that a year divisible by 400 is an exception to that rule, 2000-02-29 would be invalid

2/30/2000

Invalid date. Test to ensure that leap-year logic is functioning.

3/1/2000

This is the first day after leap-year day. The possibility exists that some part of a system may fail to recognize year 2000 as a leap year may lead to a condition where dates are no longer synchronized. Day of the week offsets can occur.

3/31/2000

First quarter-end

4/1/2000

First day of second quarter.

10/1/2000

This is the first seven-digit date with a two-digit month value. Parsing functions may fail when the number of digits representing the month changes.

10/10/2000

This is the first eight-digit date after rollover. Parsing functions may fail when the number of digits changes.

12/31/2000

The last day of the second millennia on the Gregorian calendar. The ordinal date 00.365 was the last day of 1900. Since 2000 is a leap year, its last day is 00.366. An incomplete algorithm for determining the length of the year might cause an ordinal-based system to transition into the new millennium a day too early.

1/1/2001

(Monday) This is the first day for the third millennia on the Gregorian calendar. There is a possibility of errors in computing the day of the week. Artificial intelligence system may fail ethical dilemma tests.

2/29/2004

First leap year not effected by a century or millennium transition.

4/4/2004

Stores as three sets of zeros in binary form.

12/31/2004

This date can be used to determine if normal leap years are recognized by an ordinal date system. Additionally, dates with field errors, such as a month value of 13 or the 31st day of a 30-day month should be included in test data. Out of range dates are similar in that the system should detect and reject them, but the range of dates used will depend on the system implementation.

Embedded Processes

www.nd.edu/~y2k/examples/embedded.html

The University of Notre Dame's Embedded Processes web site lists a sampling of the products in which embedded processes are used. It was posted to raise the awareness of our constituents of how pervasive the Year 2000 problem is. It has been estimated that more than 40 million embedded processes have been installed in various products over the past 30 years. Some of these are NOT date-sensitive. However, the difficulty is in determining which ones are. They are found in such diverse products as the robot on the plant floor and the processors which control a nuclear plant. They will affect such diverse products as the VCRs used in the elementary school classroom and the devices which control dangerous experiments in a university research laboratory.

Embedded processes were installed in these products to accomplish specific functions. They are of interest to Y2K problem-solvers if their functioning is dependent on dates and if they will not process these dates correctly after 12/31/99.

In some instances, it will be difficult to determine the compliance status of embedded systems, because the chip might have been supplied by one manufacturer, the board by another, the firmware by yet another, and the installation and final testing by yet another. However, because failure to find and fix Year 2000 problems in critical products will irreparably affect our lives, we must attempt to remediate as many of them as we can.

To identify embedded chip problems, answer these six questions for stand-alone (non-computer) electronic devices:

1. Does it operate with electricity? If no, the device is low risk. If yes,look further. Examples of low-risk items: tables, chairs, wind-up clocks, etc.

2. Does it have a battery or power supply? If no, it's low risk. If yes, look further. Some low-risk devices: lamps, hair dryers, electric pencil sharpeners, analog clocks, etc.

3. Does it have a display? If no, it's low risk. If yes, look further.Low-risk devices: paper shredders, power supplies, refrigerators, older microwaves, etc.

4. Does it have a microprocessor? If no, it's low risk. If yes, look further. Low-risk devices: television sets, stereo equipment, computer monitors, etc.

5. Does it have a calendar? If no, it's low risk. If yes, look further. Low-risk devices: microwave ovens, coffeepots, printers, most copier machines, etc.

6. Does the device use the calendar to schedule events? If no, it's low risk. Examples: digital clocks or calendars that don't schedule anything, cameras, watches, etc. These are low risk because operation of the device is not dependent upon an accurate calendar. The device doesn't care what date is shown; it simply shows a date. Examples of high-risk devices: phone systems, fax machines, irrigation systems, energy management systems that control lights, heat, etc., based on time and date.

These Might Have Embedded Processes

Answering Machines
Anything to do with bar codes
Call Accounting Systems (telephone)
Cars (Engine Management & Service Interval Prediction Systems
CCTV Systems
Chilled and Hot Water Systems
Computer-Bases Training (CBT) Systems
Data Chamber
Desk-Top Publishing Systems
Digital Cameras
Electronic Time Management (e.g. Personal Organizers)
Electronically Controlled Clocks/Watches
Embedded Systems (computer within "black box" from vendor)
Facilities Management System (AutoCAD)
Facilities Management Systems
Fax Machines
Fire Alarms
Flex-Clocks/Time Recording Systems
GPS's
Image Manipulation Hardware/Software (Photographic)
Kitchen Equipment
Lifts
Lighting (switching systems)
Machine Control Systems
Mobile Phones
Pagers
Photocopiers
Planned Maintenance System
Plant Control Systems (e.g. Air Conditioning)
Postage Franking Machines
Pre-printed Forms (19__)
Print Preparation software
Process Control (DCS, SCADA, RTU, etc.)
Programmable Logic Controls
Safety / Security Systems
Scientific Calculators
Security Access Control Systems
Still Camera Databacks
Stock Control Systems
Telephone System (PBX)
Telephones
Time Locks
Video Recorders
Video/Audio Editing Suites
Video Cameras/Camcorders
Voice Mail Systems
Waste Treatment Systems
Word Processing (pre-set dates)

Section 6

Sample Y2K Project Plans from Colleges

Due to the pervasiveness of computer technology and embedded chips on today's campus, the management challenge posed by the Y2K bug is substantial. Therefore, most experts consider the existence of an organized and logical Y2K project plan to be a significant factor in successfully addressing the issue at the school or campus. In this section you will find Y2K project plans meant to represent schools of varying sizes, addressing individual needs: Boston College, a medium-sized private four-year university; Salish Kootenai College, a relatively small college that is tribally controlled; the University of Iowa, a large, four-year public university. Within these plans you will find:

- A Summary of the Y2K Challenge
- Risk Assessment and Prioritization Tools and Guidelines
- The Inventory Process for Computers, Applications, Programs, Databases, and Embedded Processes
- Status Reporting Procedures
- Mistakes to Avoid
- Vendor Communications Including:

  Sample RFP/RFQ and Purchase Order Language,

  Inventory Request Forms, and

  Sample Vendor Letters

Boston College Year 2000

www.bc.edu/bc_org/fup/ia/y2khome.html

Y2K Inventory and Risk Assessment Guidelines

The Year 2000 problem will have an impact on Boston College. How much of an impact on departmental functions needs to be determined by each individual department, including all University schools, research labs, academic departments, business units, or any other functional unit. Following are guidelines that will help you complete the Y2K survey that was sent to you.

Take an Inventory

Evaluate Risk

Evaluate Other Potential Problems

Helpful Hints for Correcting Y2K Problems

We wish to acknowledge Columbia University for help in developing ideas for this web page at http://www.ais.columbia.edu/ais/html/year_2000_.html.

Take An Inventory

The first step necessary to identify potential Year 2000 problems is to take an inventory of all computers, systems, applications, and processes in your department. Review all departmental systems using **BC Hardware Compliance** and BC Softw**are Compliance links** which contain information on specific vendor products that are already Year 2000 compliant.

Keep in mind that the Information Technology Department is responsible for: (1) system software and applications on the IBM mainframe and VAX, and (2) network systems including voice, video and data. Information Technology will also provide compliance standards information for all university-wide desktop applications. B&G will review compliance standards regarding facilities management which include energy management, security, elevators, fire protection, generators, and HVAC systems.

As you begin the inventory process, keep in mind the following:

- Is the specific process critical and must the date problem be fixed or replaced to maintain department functions?
- Should the date problem be fixed before 2000? Can fixing the date problem safely be deferred until after 1/1/2000 without affecting the functioning of the department?
- Can the old program or hardware be discarded?
- Are there enough resources (personnel and dollars) in my department to fix the problem and/or purchase new hardware?
- Does data input allow for entry of a century indicator or four digit year?
- Are date displays on screens and reports in a consistent format that can be interpreted without ambiguity?
- Is date related data stored so that the century can be explicitly determined for any year?
- Will date related processing logic, i.e., calculations, comparisons and sorts, operate correctly when dealing with dates after the turn of the century?
- Will the application correctly interface with all date data that is imported or exported?
- Will date validation routines correctly validate the century?
- Will the operating system and computer hardware that the application runs in and any other system tools upon which the application is dependent (e.g., data base management systems) be Year 2000 compliant?

Inventory of computers, applications, and programs should include:

- computer operating systems, programming languages, utilities
- commercially licensed software that is not institutionally supported
- downloaded shareware/freeware
- programs or applications written or maintained by your department
- vendor-maintained applications
- shared applications, outside service providers, etc.

Inventory of databases and shared data should include:

- databases, spreadsheets, report formats, etc., maintained by your department and in active use
- data received from or sent to external sources for research, academic, or administrative purposes

Inventory of embedded processors should include:

- equipment with computers in them (lab equipment, environmental controls, access controls, security and alarm systems, chemical storage and waste management)
- anything that "knows" or records the current date or has functions based on the date

Evaluate Risk

Some processors and applications will not present a Y2K problem. For instance, some equipment may keep time of day or day of week information but not actual dates or years. Some software may already be compliant by the vendor. Some software may print date errors that can be manually corrected or ignored. All you need to do in such instances is verify that this is the case.

Be very careful about testing for Year 2000 compliance without technical assistance. In many cases, just setting the date ahead to sometime in 2000 can corrupt current data.

Appropriate solutions for your computer, applications, or processor can include the following:

- **Abandon** — no longer needed or used; not critical
- **Fix** — can be revised to handle 21st century dates
- **Replace** — can be replaced with a Year 2000 compliant replacement (if the equipment or process cannot be fixed or the fix would be very costly)
- **Defer** — need to be fixed or replaced, but not immediately

High-Risk Categories include the following:

- Any system or programs that are **unique** to your department and **support critical departmental functions or research projects**, such as applications on the desktop or on other computers that maintain date-based records for your department; use date-based data from central systems for input to your application; or produce date-based data for input to central systems.
- Local applications (written or maintained by the department) or leased ("turnkey") systems maintained by a smaller vendor. Local departmental applications are often used for decision making or planning, and therefore may have a significant business impact if not corrected. Individual researchers may use programs unique to their projects and will need to determine which of these programs are critical to their research project and must be corrected.
- Word processing programs are not likely to have problems within the software since they pick up their dates from the machine they are running on. However, spreadsheets, databases, and scheduling or calendar software should be checked for date-specific processing and date formats. It may not be necessary or urgent to fix all date occurrences if the dates are only used for displaying or printing. **However, if dates are used in calculations, sorts, or other processing, you may have to expand the dates.** For spreadsheets, this also means changing the format. Whether to fix it or not depends on how critical the process is to your department.
- Applications or programs where the original provider is unknown or unavailable. If these are critical to the functioning of your department, they will have to be reviewed and tested. If these programs or applications are not ready for Year 2000, they will have to be corrected or replaced.
- Applications that run alone or interface with other applications or programs such as the IBM mainframe or other systems external to the University. Also, determine whether the interface is compatible.
- For data received or downloaded from IT-supported systems, or from an outside vendor, determine the provider's Year 2000 solution so that your programs can be modified to accommodate the necessary changes.
- For shared data, coordinate the appropriate Year 2000 solution with your partners.
- For PCs, you may have a problem with dates stored in the hardware basic input/output system (BIOS). BC's Hardware Compliance link will identify all hardware models purchased through BC's computer store or delivered through the departmental replacement process that are Y2K compliant. If you have an older PC that you plan to use after the millennium, the BIOS should be checked for compliance for high-risk systems. Information Technology will be providing more information on BIOS testing and correction at a later date. The internet has much information on this topic, **however, be very careful about testing for Y2K compliance without technical assistance.** We heard one story about an individual who replaced his BIOS board and blew out his older monitor from the electrical surge of the new board.

Evaluate Other Potential Problems

Embedded Chips

One of the largest unknown and least understood areas in Year 2000 evaluations is the effect of the century rollover on equipment with embedded microchips that may retain, record, or react to dates and/or elapsed time. Evaluate any equipment, system or processor which "knows" the date, records it, or functions by date control. Whenever possible, contact the vendor or manufacturer of such equipment to determine whether the equipment is Year 2000 compliant or if the vendor has a later model which is. Examples include:

- environmental control systems
- access control systems
- lab, clinical, and other monitoring equipment
- automated date/time stamping equipment
- chemical storage/waste management systems

Preprinted Forms

Another area to consider, although not a high-risk category, concerns any preprinted form you may have. When reordering forms, check for any date issues.

Helpful Hints For Correcting Y2K Problems

The specific measure for correcting Y2K problems will vary from department to department, depending on the problems identified in the risk analysis. For department generated applications, scheduling fixes and performing tests should be based on the criticality of specific processes and applications. Date-sensitive processes and applications essential to the research, academic or administrative functions of the department should be addressed first.

- There are two primary software solutions for Year 2000 compliance: expansion and windowing.

  Expansion
  In expansion, all date fields are redefined to contain four digits for the year and any affected coding is modified accordingly.

  Windowing
  In windowing, only the coding is changed. Two-digit years greater than some cutoff date are assumed to be 20th century; years less than the cutoff date are assumed to be 21st century. (For example, if the cutoff date is "39", the date 1/15/40 would be treated as 1/15/1940. The date 1/15/38 would be treated as 1/15/2038.) The size of date fields in databases, etc., is not changed.

Different vendors can use either solution. Be sure you know what their particular software solution is and what effect it may have on your application.

- Wherever applications share data or interface to other systems, it is important to know what solution has been chosen for Year 2000 compliance. For instance, if Program A has been expanded to include 4-digit years in all date fields, but receives input data from Program B which is using "windowing" (2-digit years), then the data must be expanded on receipt or Program A will fail or produce incorrect results.
- Spreadsheet and database Y2K compliance suggestions are as follows:

Spreadsheets:

- identify the spreadsheets using cells with dates
- find out the information source (manual input, link/feed, system date)
- find out vendor (MS, Lotus, WP, Borland) recommendations for dates
- review how dates are used and decide how dates will have to be changed
- increase column widths for each spreadsheet where a four-digit year is needed
- check reports and resize the dates to four-digit year where needed format date as mm-dd-yyyy
- review macros and formulas that use dates and change where needed

Databases:

- identify date fields in all databases
- find out the information source (manual input, link/feed, system date)
- find out vendor (MS, Lotus, WP, Borland) recommendations for dates
- increase date column widths as necessary
- document the date changes and communicate them to all users
- adjust column width and type size in reports, where necessary
- recompile and make program changes, where necessary
- test changes

- Be sure to update all user manuals, help files, and documentation to reflect any changes, especially if the change means differences in the way dates are entered into the application, or if interfaces to other application are modified.
- For critical applications, think about creating a contingency plan (i.e., can I perform the process manually?)
- It is essential to take backups of data and programs prior to any conversions or testing. These backups may be needed if you encounter problems with your conversion efforts and need to back out your Year 2000 changes.

END USER APPLICATION SURVEY FORM

Please complete one sheet for each unique computer application, control system, tools developed or acquired, or standalone non-standard or BC-supported systems used in your department or organization that store, manipulate, calculate, compare, sort date information, or periodically report information to sources internal or external to your organization)

Date: _____

Department: _____

Form Prepared by_____

Position: _____

Application or
Product Name: _____

Version #:_____

Release Date:_____

Manufacturer or creator of the application:
_____

Vendor Contact Name (if known):
_____

Vendor Contact Phone # (if known):
_____

Purpose of the application:_____

Importance to your department or organization:

1. extremely important
2. somewhat important
3. not important

Where does the application reside?

1. LAN server
2. desktop
3. Unix mid-range computer
4. Other_____

Year 2000 compliant? ❑ Yes ❑ No If "No", expected date of compliance:_____

Leap year compliant (i.e., will leap year 2/29/2000 be recognized)? ❑ Yes ❑ No

Internal systems that your application interfaces with (i.e., data uploaded to IBM mainframe, etc.)

1. _____
2. _____
3. _____
4. _____

Has the application or product been tested for Y2K compliance? ❑ Yes ❑ No

Does the application create data or reports that are used by anyone outside your department? ❑ Yes ❑ No
If "Yes", who:

1. _____
2. _____
3. _____

Is the application dependent on data inputs from outside your department? ❑ Yes ❑ No
If "Yes", from where:

1. _____
2. _____
3. _____

How many individuals use this application? _____

What is the potential impact of failure of the application?

1. no impact
2. some impact
3. great impact

How does the application interface?

1. LAN connection
2. sharing of diskettes
3. other _____

How often is the application executed?

1. daily
2. weekly
3. monthly
4. quarterly
5. annually

Which computer operating system is used?

1. DOS windows
2. Unix
3. Mac
4. Other_____

Do you anticipate that funds will be needed to replace your current system? ❑ Yes ❑ No

If "Yes", indicate amount: $_____

Do you use EDI? ❑ Yes ❑ No

If "Yes", with whom do you exchange data?
_____

Do you use FTP to exchange data? ❑ Yes ❑ No
If "Yes", indicate:

1. on-campus
2. off-campus
3. both

Salish Kootenai College, Pablo, Montana

Management Plan for Year 2000 Technology Compliance

Overview

Salish Kootenai College (SKC) has been monitoring and addressing Year 2000 (Y2K) compliance issues since 1996. These efforts include all aspects of electronic technology used at SKC including microcomputers, servers, telephony equipment, network devices, microcode, embedded systems, printers, and software systems.

The highest priority for evaluation at SKC are administrative computer systems, servers, network devices, and mission-critical software. Failure of these systems would create enormous problems for SKC, staff, students and other institutions who deal with SKC.

Ongoing activities

SKC has, and continues to use, many tools and techniques for verifying Y2K compliance. These include by order of use: vendor specifications, software evaluation tools, testing, interviews with users of technology, and software auditing. The results of these evaluations are noted in an inventory-based, help-desk application to track progress. As items are evaluated their status is noted as compliant, compliant with modifications, or not compliant. Items that are compliant with modifications are brought within compliance. Items that are not compliant are evaluated to determine if they can be used for services that do not require compliance or replaced.

As software is reinstalled systems are reverified for compliance and the appropriate patches or revisions are reapplied.

Y2K compliance status

All mission-critical resources have been verified to be Y2K compliant or compliant with modifications. This includes administrative computer systems (financial, student services, etc.), servers network devices, and mission-critical software. All current modifications, such as patches or new versions, have been loaded and tested. Since this status can vary as new systems are brought on-line, this is a continuing activity.

The Network Administrator maintains extensive records and vendor information packets which address Y2K compliance.

SKC has a large number of Apple Macintosh computers both administratively and academically. All of these units are Y2K compliant.

Recent purchases (for the last 18 months) of Intel-based systems have been verified as Y2K compliant.

Census software has been installed on all microcomputers to monitor installed software. This is used to validate against vendor standards for Y2K compliance.

Most administrative, Intel-based systems with older BIOS have been patched using several software tools. Less than five units have been identified as non-compliant

Users of non-compliant technology products are notified when evaluation is completed.

Users with non-compliant applications, or documents such as databases, are notified as encountered.

Results of Y2K compliance checking

SKC is comfortable it has addressed all major Y2K issues. All mission-critical systems have been tested, validated, and patched if necessary. A process is in place to continually monitor Y2K compliance as new hardware arrives, software is reinstalled, or additional Y2K issues are made available by vendors.

All Macintosh based systems are Y2K compliant. Since staff and faculty either use Macintosh or newer Intel-based systems over 98% of staff and faculty systems are Y2K compliant.

The primary area of work for 1998 is validation of academic, Intel-based systems used in student labs. The numbers of computers that fit into this category, and are either compliant with modifications or non-compliant, are under 30 (less than 10% of the installed units.)

Riding the Technology Buffalo

Ideas to Help Survive the Millennium (Year 2000) Bug

Background

By now, most people have heard about the Year 2000 (Y2K) problems that revolve around the use of two digits to represent years. When 2000 rolls around many computers, VCRs, microwaves, wristwatches, electrical generation facilities and a host of other technology systems may not be able to distinguish between 1900 or 2000. To add insult to injury, 2000 is a non-standard leap year (a leap year is added every 1000 years) and many devices may not function properly on February 29, 2000.

How much impact the Y2K bug will have on humanity is uncertain and includes doomsday prophets who have withdrawn all their savings and moved to Montana to live in a solar-powered cabin in the mountains. At the other end of the spectrum are people who think there will be only nominal problems because programmers and others are busily fixing Y2K issues.

The Process

Between these two vastly disparate visions are the Tribal Colleges who will address any potential problems with the millennium bug in different ways. As with other problems that affect Tribal Colleges, there is a need to accomplish the following, basic tasks:

1. **Identify and understand the threat**
   The threat is the Y2K bug.

2. **Identify the resources affected by the threat**
   The threat can affect any technology, embedded device, or data storage mechanism that uses a date to operate or calculate. Some examples of potentially critical systems at Tribal Colleges include:

   a. Computer systems.
   b. Software such as databases spreadsheets, training software, etc.
   c. Embedded control systems such as thermostats, postage machines, etc.
   d. Telephone systems, faxes, video-conferencing, etc.
   e. Administrative software systems (Financial Aid, Business Office, Registrar, etc.)
   f. Outside vendors including utility companies, telecommunication services, State government and Federal government
   g. Operating system software (such as UNIX, Windows95, or MacOS)

3. **Prioritize the identified resources and their impact to the Tribal College**
   High on the list for most Tribal Colleges is item e, Administrative Software Systems. Impacts on these systems will probably occur before 2000 as students will be registered and budgets will be setup for the 1999-2000 academic and fiscal year.
   The central issues are:

   a. Can you register students?
   b. Can you process and award financial aid?
   c. Can you accurately count ISC?
   d. Can you accurately produce reports such as IPEDS, for the government or to meet grant reporting obligations?
   e. Can you process payroll and produce reports such as W2s?

4. **Identify financial and technical resources to address critical issues**
   This will be the most difficult part of the process. If the Tribal College has not yet begun to look at Y2K issues it may be too late to avoid some problems.

5. **Fix the problems**
   There are software applications that can patch computers to allow them to cross the Year 2000 boundary with minimal or no problems. Some computer companies have integrated circuit chip replacements (BIOS) to allow computers to continue functioning. These chips generally cost $60 per computer. Some computers and other technology systems may not operate at all due to timing issues related to internal timing and communication with peripherals.
   Software applications and operating systems often have patches to fix problems. Most popular business systems have Year 2000 compliance information packets on their web sites. Testing is the only sure method for ensuring compliance.
   Databases, spreadsheets and other documents are the most difficult and troubling problem because finding and fixing date-based information is quite time-consuming and costly.

6. **Monitor compliance before and after 2000**
   Year 2000 problems will continue after 2000 as new hardware, software and other technology systems are installed at Tribal Colleges. As mentioned above, February 29, 2000 is the next critical day.

7. **Hope for the best and plan for the worst**
   TIME recently published an article explaining that the millennium bug will have far less impact than the mainstream press seems to be pontificating. If the primary systems a Tribal College relies upon for its survival then the Tribal College will be able to survive with more or less problems in the periphery that can be fixed with time and funding. The great unknown for most Tribal

Colleges will be how external vendor's Year 2000 compliance will affect Tribal Colleges:

a. Are you able to draw down funding as needed?
b. How will you handle bills for millions of dollars because interest was calculated from 1900 instead of 2000?
c. Can you potentially survive with delayed telephone service?

Summary

There are many books, periodicals, articles and Internet resources which discuss issues related to the millennium bug. Reading a variety of these articles can help sort out what is important for Tribal Colleges. Each Tribal College will take a different path in dealing with Y2K problems. For some, who depend more heavily on technology for day-to-day operations, the Y2K problem is very important and critical to address. For others, who still process registration and financial aid on paper, they will have fewer impacts. Since most institutions do some financial processing on computers, this will be the most common and critical issue for Tribal Colleges. The remaining problems, which won't be fully known until January 2000, are related to interoperability with vendors, State and Federal government.

Resources

Salish Kootenai College is developing an Internet-based class to help Tribal College personnel deal with the millennium bug. Other institutions and vendors have courses, books, teleconferences and other resources which provide information and suggestions on how to deal with Year 2000 issues. Following are several Internet URLs for sites that discuss Y2K problems and solutions:

Year 2000 Web Sites

Informational Web Sites

http://www.year2000.com/
General Y2K Information

http://www.euy2k.com/index.htm
Y2K Information on Utilities

http://www.itrain.co.uk/fry2mbon.htm
Briefing on Y2K Problem

http://www.csis.org/html/y2ktran.html
Center for Strategic & International Studies Y2K Site

http://www.comlinks.com/
General Y2K Information

http://www.boxwareinc.com/whytfnt.html
Explanation why Windows NT may need Y2K fix

http://www.yardeni.com/
Dr. Ed Yardeni's Economic Web Site

Company Y2K Web Pages

http://www.microsoft.com/technet/topics/year2k/default.htm
Microsoft's Y2K Site

http://www.cisco.com/warp/public/752/2000/index.shtml
Cisco's Y2K Site

http://www.novell.com/year2000/
Novell's Y2K Site
Novell announced that 4.1 will have Y2K patches available by Q4 1998

http://www.dell.com/year2000/index.htm
Dell Computers Y2K Site

http://www.compaq.com/year2000/index.html
Compaq's Y2K Site

Hub Sites

http://www.yahoo.com/Computers_and_Internet/Year_2000_Problem/

Inventory

Hardware Inventory

A hardware inventory was completed this summer. A database was developed from this inventory categorizing the computer systems at SKC into one of eight different configurations.

These configurations detail whether the hardware BIOS and Operating System are Y2K compliant.

Software Inventory

A software inventory was complete this summer. A database was developed containing information whether the software had any Year 2000 issues.

Vendor Query

A query of vendors, both hardware and software, concerning their productΔs Y2K status was started this summer.

This is an on-going process which will continue until well after Year 2000.

This query is being added to the hardware and software databases noted above.

System Audit

Based on the inventory above a more in-depth inventory was conducted on the non-compliant hardware, Operating Systems, and software applications.

Testing is being currently conducted on various Operating System and software application configurations to determine if fixed implemented below have corrected Y2K problems.

Discussions are on-going with college staff as to the Y2K status of the various databases, spreadsheets, etc. that they use, and as problems are found the staff are aided in correcting them.

Implementation of Y2K Fixes

Based on the Inventory and audit several types of fixes where decided upon.

Patches for Microsoft Operating Systems, i.e. Windows 95, Windows NT, and Windows 3.1, were downloaded and installed.

This part of the project nearly complete

Patches for Novell Netware were downloaded.

The software has not yet been installed on the servers.

Patched for various software applications are constantly being downloaded and implemented.

Ongoing until after Year 2000.

A software program that installs at startup on the PC's was purchased to correct the Y2K problem on non-compliant hardware systems.

This program has been installed on all of our non-compliant PC's in service.

Updated BIOS chips were purchased for one of our PC labs which corrected Y2K problems. The chips were purchased because larger hard drives were installed and the old BIOS did not support them. Installing the BIOS chips solved two problems.

Based on the Inventory and audit, a plan of attack was developed and implemented.

Basic Plan Outline

Prioritize systems based on usage

SKC Servers

Staff computers were targeted first

Computers Labs were targeted next

The necessary Y2K patches (both BIOS and software) were applied.

Some systems, such as our Novell servers have yet to have patches applied because we are waiting for vendor fixes.

Testing of Y2K patches is currently being completed

Various application software and Operating Systems combinations are being tested.

Some examples

- Windows 95 and the various programs used in our Nursing CBT program.
- ClarisWorks on older OS Macintoshes
- FirstClass Email server
- Appleshare Server
- SMTP Email gateway
- EIMS Email gateway
- Webstar Web server

This testing involved several tests including:

Manually setting clock to December 31, 1999, 11:59 pm; shutting the computer off, wait 1 minute, restart, check the OS clock and various software applications to assure the rollover to the Year 2000 worked correctly.

Manually setting clock to February 29, 2000 and check the OS clock and various software applications for correct date/time.

This testing will continue until the Year 2000.

On-going Vendor research

This research, ie checking with hardware and software vendors for Year 2000 issues concerning their products, will continue until after the Year 2000.

UI Toolkit 2000

www.uiowa.edu/~Team2000

Guidebook with Assessment Tools and Resolution Strategies for the Year 2000 Technology Challenge

"The issue of year 2000 compliance requires our urgent attention. We have an excellent plan for updating central systems such as payroll and student records, but departments are responsible for reviewing their own internal systems and processes. This means each department must begin immediately to review manufacturers' specifications or test equipment and software for century-specific elements, and determine the budget consequences of assuring functionality into the next century."

- President Mary Sue Coleman

AUTHORED BY: SCOTT ARNESON, SUSAN BECKETT, DONETTA BOONE, RICK BORCHARD, CHARLIE DRUM, BRUCE JOHNSON, TERRY JOHNSON, DOUG LEE, SUE NICKELS

Contents

1. What exactly is the Year 2000 Problem?
2. Problem scope and impact
3. Prioritizing of risk
4. Assessment tools and resolution strategies
5. Status reporting procedures
6. Contact points *(not included here)*
7. Appendices
   - **A** RFP, RFQ and Purchase Order year 2000 language
   - **B** SAID inventory request form
   - **C** Definitions of SAID inventory elements
   - **D** Definitions of blank assessment fields
   - **E** Sample Report - Electronic file format *(not included here)*
   - **F** SAID Inventory Report - Non-electronic format *(not included here)*
   - **G** Sample vendor memoranda
   - **H** Monthly report to Team 2000

What exactly is the Year 2000 Problem?

The Year 2000 Problem, also known as the "Year 2000 Bug," actually is an entire category of date-related issues that will affect equipment and computer systems. Easy to understand but very difficult and time consuming to detect and correct, the Year 2000 Problem is payback for a shortcut programmers took years ago to save on limited and extremely expensive computer memory space. (Would you believe that in 1963, one megabyte of hard disk space cost $2,000? Today, it costs less that $1.) Trouble is, the shortcut never got changed and the clock keeps on ticking into the next century.

The problem is that many computerized operating systems and applications (and the software inside that tells them what to do) are programmed to use a standard two-digit year field MM/DD/YY where YY represents the calendar year.

For example, a computer would write January 1, 1999 as 01/01/99. But unless something's done, when the year 1999 rolls over to 2000, many systems that use the two-digit year field will interpret the first day of the new year as 01/01/00, and assume that "00" means 1900—reading "00" as coming before "99" in numerical sequence.

You may ask why this problem has never before occurred. Benjamin Franklin's famous kite experiment took place in 1752, and Thomas Edison perfected the light bulb in 1879. Iowa State University developed the Atanasoff-Berry Computer during the years from 1939 to 1942. You can see that although the evolution of electricity has taken several hundred years, the storing and manipulating of data in an electronic fashion has never before crossed a century boundary.

More than just a computer problem

Because the Year 2000 Problem has the potential of affecting all electronics-based technologies, it threatens many aspects of what we do on a daily basis communications, services, instruction and research.

Although the most obvious areas of concern are computers, the Year 2000 Problem is more than just an IT (Information Technology) or computer issue. It also can affect a long list of systems and equipment with embedded microchips that are used in the workplace and in our everyday lives.

Not all devices use software to function. Many devices essential to doing business – fax machines and photocopiers – use computer chips. For instance, devices that need to be checked within the University include programmable heating and cooling systems in buildings, security systems, vehicles and voice-communications systems. If a device has a printed circuit board, it is likely to have a computer chip and to have the potential for a Year 2000 Problem.

Glitches may occur sooner

The Year 2000 Problem does not necessarily kick in the moment the clock strikes midnight on December 31, 1999. Some credit card, home mortgage and insurance companies already are seeing their systems malfunction when an expiration date of "00" is issued.

Awareness is crucial. To that end, the project team has developed and initiated a comprehensive communications plan to get the word out to employees and students about the Year 2000 challenge.

Because many functions critical to a university rely on the effective processing of dates, time is of the essence!

Who is responsible for solving the problem?

Although experts do not agree on the seriousness of the problem, we are taking the mere threat of such operational concerns very seriously. That is why Team 2000, headed by

Sue Nickels, was formed to coordinate the University's assessment and resolution efforts.

The team's primary objective is to develop and implement a University-wide project plan designed to mitigate the Year 2000 Problem and make sure all of our equipment and systems are Year 2000 compliant – able to process all date sequences without complications.

Ultimate responsibility for Year 2000 compliance rests with each one of us!

Now for the good news!

The Year 2000 compliance status of certain equipment and software on campus is being addressed centrally.For instance, Facilities Services is researching the controls over the elevators, fire alarm, and smoke detectors in your building. ITS (Information Technology Services) and HIS (Hospital Information Systems) are checking on mainframe applications, operating software and related hardware. They are also assessing the impact to the Local Area Networks and telecommunications equipment within their purview. UI's Purchasing Department has added language to RFPs (Requests for Purchase), RFQs (Requests for Quote) and POs (Purchase Orders) which requires vendor certification of Year 2000 compliance so that your normal purchasing cycle will not be disrupted. Please see Appendix A for this language.

Of course, you still have responsibility for the bulk of the at-risk equipment and systems which fall within your organization, department, or unit. And now the bad news:

- If you lease or rent at-risk equipment, you will need to establish its compliance status as well.
- If you routinely use vendor-supplied electronic ordering systems, data retrieval systems, or other electronic communication links, you will need to assess how Year 2000 might affect those activities.
- If you rely on external vendors for critical software/hardware maintenance, you will need to ensure that the vendor is still capable of providing timely service once the Year 2000 arrives.

The list is virtually endless but the time frame within which we must all work is not. The need to identify and prioritize risk associated with the Year 2000 is paramount.

Problem scope and impact

Anything that is electric or battery-powered and is date-controlled, -driven, or calculated could be affected by the Year 2000 Problem.

Computer hardware includes such things as mini-computers, local area and wide area network equipment, personal computers, printers, and accessories. The compliance status of hardware supported by ITS (Information Technology Services) or by HIS (Hospital Information Systems) will be addressed by ITS and HIS staff.

Computer software includes operating systems, commercial software applications, and any locally developed applications software. Locally developed software does include such items as MSAccess, MSExcel, or SAS programs created by staff within a departmental or operating unit office. ITS and HIS staff will address software supported by ITS or HIS.

Instructional equipment includes VCRs, classroom personal computers, projection equipment, and any other electronic instructional support equipment or software.

Scientific and technical instruments are such items as diagnostic or scientific equipment that measures mass/density, radiation, wavelength, temperature, or time, and technical equipment used in the manufacturing or maintenance of other equipment or products. Related diagnostic and calibration software is also at risk.

Medical equipment and instruments are such items as diagnostic or therapeutic medical equipment and related software. Software that provides archival data storage and retrieval is also of concern.

Communications and office equipment includes voice and data communications items like switchers, routers, bridges and concentrators. At-risk office equipment includes fax and copying machines, automated safes and vaults, and time-reporting devices such as time clocks or punch clocks.

Building mechanicals includes heating/cooling regulators as well as security systems, alarms, and other safety devices. Potentially at-risk items for review are security or mechanical devices that detect motion, sound, light or temperature fluctuations, and emergency control devices that may trigger an automated emergency call (911 or UI Public Safety). Elevators, automated lighting systems, electronic vending machines, keyed access devices or continuous current monitors must also be reviewed for compliance.

Transportation systems are those UI vehicles (automobiles, vans, trucks, buses and ambulances), owned or leased, which may be equipped with computer chips. Also included in this category are fuel pumps and diagnostic devices used in servicing or repairing vehicles.

Other refers to electronic equipment and devices not captured by the categories above.

Prioritizing Risk

Risk Categories

The most important thing you need to think about when addressing the Year 2000 Problem for your work environment is risk of failure: What are the organizational and personal consequences if this system, process or equipment item is noncompliant? Here is a simple way of prioritizing noncompliance risk:

Life-threatening failure could result in human death or injury.

Mission-critical	failure could be disastrous to your operating unit, UIHC, or the University of Iowa.
Priority	failure could have substantial impact on your operating unit, UIHC, or the University of Iowa.
Non-priority	failure could result in trivial costs or only inconveniences.

Life-threatening and mission-critical systems, processes, and equipment items must be your first concern. Identify and evaluate items in these two categories as soon as possible to eliminate risk of failure.

Definition of Compliance

What does it mean for a system, process or equipment item to be compliant? The State of Iowa defines Year 2000 compliance as meaning that the system, process or equipment item shall:

- Identify and process date and time data without causing any processing interruptions, abnormal terminations or changes in performance level, characteristics or functionality; and
- Identify, process and manipulate all date and time data related functions correctly (including leap year calculations, day-in-year calculations, day-of-the-week calculations, and week-of-the-year calculations); and
- Correctly handle date and time related data, before, on, and after January 1, 2000, including but not limited to accepting input, providing date data output, and performing ongoing operations on dates and portions of dates, including but not limited to calculating, comparing and sequencing of dates (in both forward and backward operations spanning century boundaries); and
- Correctly store and provide output of all date and time data in a manner that is unambiguous as to century.

Mistakes to Avoid

One large banking organization in Texas listed the top mistakes organizations are making in addressing the Year 2000 Problem:

- **Denial –** Thinking that the problem does not exist or if it does exist, it doesn't affect them.
- **Wishful Thinking** – Thinking that someone is going to come up with a "silver bullet" that magically makes the problem go away without too much trouble or expense.
- **Putting on Blinders** – Thinking that solving their own internal Year 2000 compliance problems is good enough, not realizing that if their vendors, suppliers, or customers fail, then they may fail also.

Assessment tools & resolution strategies

Mobilization strategy and timeline

In order to accomplish the monumental task set before us, Team 2000 has designed a reporting process which is more fully described in the next section. Before embarking on the reporting process, an evaluation must be completed by each Org Unit. Team 2000 recommends the following strategy:

Step 1: Organize local assessment team and develop preliminary completions timeline.

Step 2: Identify and prioritize "at risk" systems, processes and equipment items. This will be an ongoing process which can begin with "SAID" inventory data for your operating unit.

Step 3: Assess compliance status and formulate a resolution plan for life-threatening and mission-critical systems, processes and equipment items. This will also be an ongoing process as you identify equipment and assess risk.

Step 4: Implement resolution plan for life-threatening and mission-critical items. At the same time, assess compliance status and formulate a resolution plan for priority systems, processes and equipment items.

Step 5: Implement resolution plan for priority items. At the same time, assess and resolve non-priority systems, processes and equipment items.

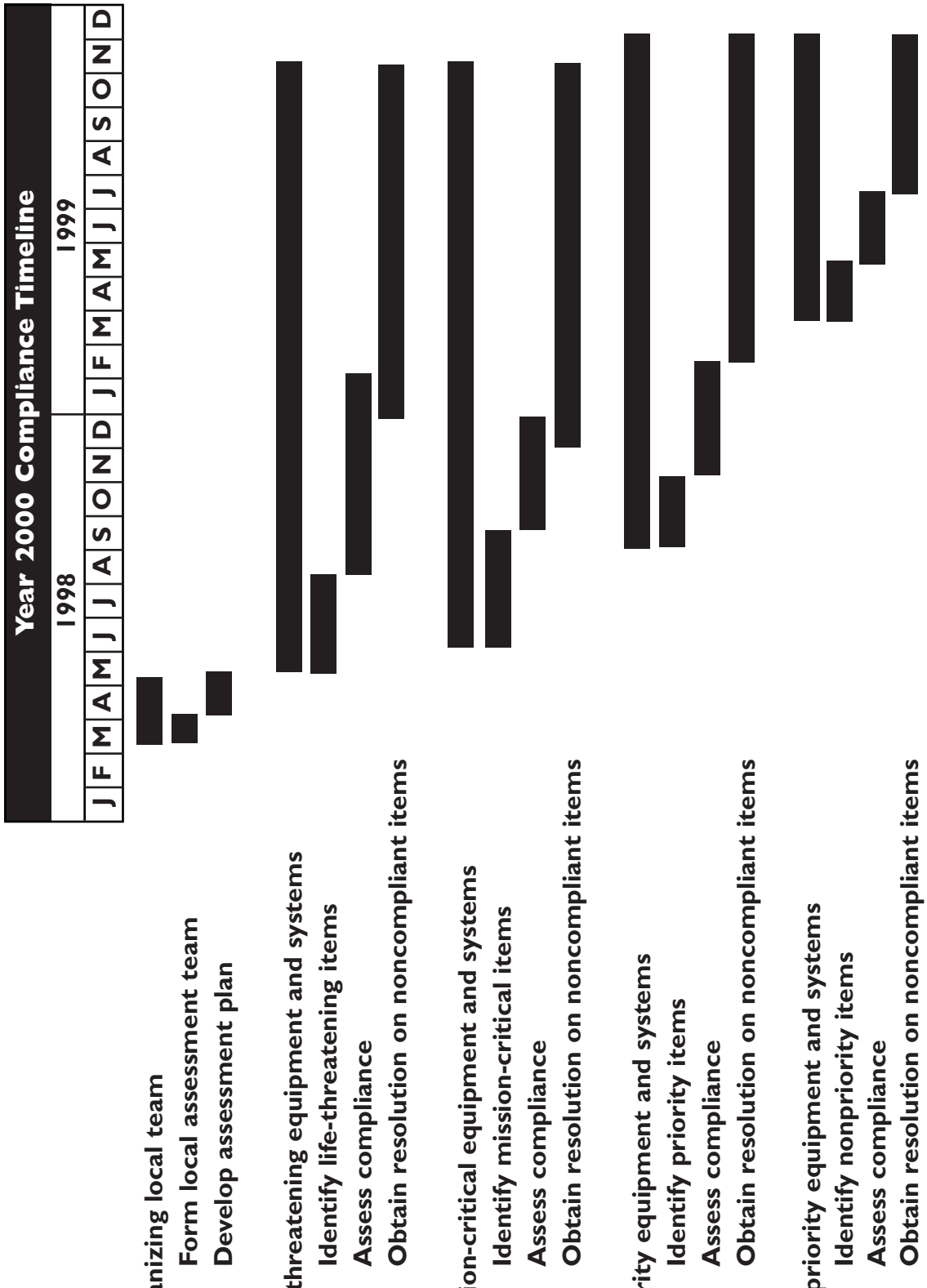
Aids for identifying equipment

Team 2000 can provide University of Iowa entities with their inventory data from the mainframe "SAID" equipment inventory system. This data is a starting point for evaluating your equipment for Year 2000 compliance. The data you receive will include fixed asset inventory items from SAID, which were purchased prior to January 1, 1998. The process attempts to automatically remove things like desks, chairs, tables, credenzas and books from this beginning inventory.

Warning: This list should not be considered complete. Items which are not covered by this initial inventory list but which you and your staff should consider when reviewing your Year 2000 vulnerability include:

- **leased equipment**
- **software**
- **critical services supplied to you by others** (for example: Maintenance for mission critical equipment may be dependent on software or hardware which may contain components affected by the century change. If such equipment fails, the UI could be without adequate maintenance or equipment diagnostic testing for critical items.)
- **new purchases not reflected on the SAID database** (these include any purchases after Jan. 1, 1998)
- **purchases falling below the SAID capitalization threshold** ($500 prior to 7/1/97; $2,000 beginning 7/1/97)
- **financial or any kind of electronic transaction with an outside service** (this would include information we are sending to or receiving from another institution, business or vendor)

Year 2000 Compliance Timeline



- **vendor ordering devices** (for example: A department may order supplies from a company via vendor supplied ordering devices. Should these ordering devices fail after Dec. 31, 1999, critically needed orders may not be transmitted to or received by the vendor.)

SAID inventory data request

To request this data, either complete and electronically submit the inventory request form found on the SAID Inventory Request Form, or print the form, complete the information requested on the form, and mail to ITS Setup & Operations, B4, JH.

You may request raw data or you may request a printed inventory listing or you may wish to receive both.

SAID inventory data delivered

The electronic data received from the SAID inventory system must be imported into a software package of your choice for review and manipulation. This raw data will contain the fields of information as presented in Appendix C.

The electronic data returned to you will include eleven fields of blank information. These have been prepared for you as a "template" for completing your Year 2000 review and are described in Appendix D.

Inventory recommendation

Team 2000 recommends the electronic data option to facilitate the evaluation process. By storing the data in a software package such as MSAccess, you may delete inventory items having no electronic components, you may sort items by building or person responsible for distribution to those performing the assessment function, and you may add data to the blank template fields as your review of equipment progresses.

After reviewing your work environment for Year 2000 vulnerability, we hope you will prepare your FY98-99 and FY99-00 budgets bearing in mind any required Year 2000 corrections. Departments will be held responsible for the costs required to upgrade or correct for this technology defect.

Ideas for Assessment

Team 2000 members have surfed the web and found numerous vendor statements pertaining to Year 2000 compliance. These links may be found within the Team 2000 home page: **http://www.uiowa.edu/~Team2000**

If a link is not currently available for the device or software you are assessing, we recommend the following:

- Search the web for information. If you find what you are seeking, and determine it is valuable information, send an e-mail to uiteam-2000@list.uiowa.edu and ask for the link be added to our homepage.
- Submit a question to the campus listserve (uiyear2000@list.uiowa.edu) describing the specifics of the equipment you are researching. Or, submit a question to a professional listserve to which you subscribe to determine if any colleagues have Year 2000 information relating to your device or software.
- Contact the vendor or manufacturer using either of the sample memoranda shown in Appendix G to request compliance information. The nature or use of the equipment may influence which of the two memoranda you would like to use. For instance, reviewing the compliance of life support equipment may be better served by Memo 1, and the compliance of a printer may be established by Memo 2.
- Perform a test yourself on the equipment or software. This is highly recommended if it has been categorized as life-threatening or mission-critical.
- Plan to replace the item before it fails if you fear there is no other resolution.

Potential Resolutions

Available resolutions may include a remedy provided at vendor cost, a remedy resulting in additional cost to the department or operating unit, replacement as a part of the normal life-cycle of the equipment, or work redesign causing the non-compliant device to be unnecessary.

Status reporting procedures

The President and Vice Presidents have charged Team 2000 with collecting information from the campus regarding assessment, resolution and estimated cost to remedy systems impacted by the millennium change. To accomplish this goal we are requiring completion of the "MONTHLY REPORT TO TEAM 2000" form. This form is not available on the web, but you may request an electronic or printed copy from Sue Nickels.This form should be updated and submitted to Sue Nickels, Project Manager-Team 2000, ITS, 400 NWB, no later than the fifteenth day of each month.

The report is in matrix format whereby you identify the level of risk and category for each particular piece of equipment owned, rented or relied upon by your area. For each category and risk level, you are expected to provide a percentage complete with respect to the identification and assessment of the problem; a percentage complete for resolving any problems; and, an estimate of the cost to be incurred by your area in upgrading or replacing existing equipment or systems in order to be year 2000 compliant.

Completion of this form will require a full assessment of equipment owned or rented by the University. In addition, consideration must be given to system interfaces where the University utilizes an external system to conduct business processes or functions (ex: an ordering system supplied to us by the vendor).

Definitions regarding categories of equipment can be found in the "Problem Scope and Impact" section. Definitions regarding level of risk can be found in the "Prioritizing Risk" section, and in Appendix D under "classification".

APPENDICES

Appendix A
RFP/RFQ and Purchase Order Language

The UI Purchasing Department prints the following text on all Requests for Purchase (RFP's) and Request for Quotes (RFQ's):

Does vendor guarantee and warrant that the equipment being proposed is Year 2000 Compliant and will be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000.

YES _____ NO _____ (Vendor Must Check One)

Your response will be considered during the evaluation of the bid.

Vendor's failure to check a response may result in automatic rejection of the bid.

The UI Purchasing Department prints the following text on all Purchase Orders:

By accepting and delivering product on this Purchase Order, the vendor warrants that the product(s) being provided will be Year 2000 Compliant and will be able to accurately process date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the year 1999 and 2000. In the event that the delivered product(s) is not Year 2000 Compliant as set forth in this paragraph, and in addition to any remedies available to Buyer, Seller expressly agrees to replace or repair the delivered product to Buyer's written satisfaction, and in any event to provide Buyer with delivered product which is Year 2000 Compliant within 30 days of written notice from Buyer that the delivered product originally provided to Buyer under the terms and conditions of this Purchase Order is not Year 2000 compliant.

Appendix B
SAID Inventory Request Form

Request via the web: SAID Inventory Request Form

Section One

Name: _____

Email: _____

Campus Mail Address: _____

Campus Phone Number: _____

Dept Name	Dept MFK#	SubDept Name	SubDept MFK#

(You may either enter a department MFK, or both a department and sub-department MFK)

Section Two

Do you wish to receive a delimited file ❑ Yes ❑ No (If no, go to Section Three)

File name where data is to be stored:	
	(maximum of 8 characters: numeric and alpha characters only)
Field delimiter character:	❑ Tab ❑ Comma
	(tab for MS Excel, comma for MS Access)

Section Three

Do you wish to receive a printed report?

❑ Yes ❑ No (If "no", press submit)

Beware: this could be a massive amount of paper!

Select one option as the sort order of your report

❑ Department/SubDepartment/Person Responsible/UI Tag Number

❑ Department/SubDepartment/Assest Class/UI Tag Number

Please fill in the form completely, and send to ITS Setup & Operation, B4,JH

Thank you for preparing for the Year 2000!

Appendix C
Definitions of SAID inventory elements

Asset ID: Number assigned to an asset to differentiate that asset record from any other asset in the SAID database, usually the Asset or Tag number.

Asset Number: The University of Iowa tag number assigned, and affixed to the physical asset.

Description: Short descriptive text of the asset.

Class: Classification of assets as to type or grouping of like assets, i.e., desk, computer, etc.

Building: The building in which the asset is located.

Room: The room in which the asset is located.

Person Responsible: The last name of the person having responsibility for the asset, or to whom the asset is assigned.

Person Responsible 1st Init: The first initial of the first name of the person having responsibility for the asset, or to whom the asset is assigned.

Serial #: The manufacturer's number assigned to the asset to identify that asset from all others.

Maint #: Any number assigned by a "vendor" which identifies a maintenance agreement for the asset.

Model #: A number, assigned by the asset manufacturer, which specifically identifies the asset according to a unique group of specifications.

Acquired Date: Date on which ownership transferred to the University of Iowa

PO#: The Purchase Order number which covered the purchase of the asset.

Vendor #: The Accounts Payable and Purchasing system number, identifying the vendor from which the asset was purchased.

Department: The department identifier (number) indicating the ownership or assignment of the asset. As per the Accounting Code Manual, a department is "a reporting entity defined by the Board of Regents or administration to meet the specific reporting requirements of the University of Iowa."

Sub-department: The sub-department identifier (number) indicating the ownership or assignment of the asset. As per the Accounting Code Manual, a sub-department is a "sub-element" of the department. It allows a department to separate financial information into more detail. Some organizational units have named the combination of the department and the sub-department the responsibility center. A department may use the same sub-department number set up by another department, because the system validates the combination of these two elements as one.

Asset Value: The acquisition cost or the appraised value at point of gift of an asset.

Appendix D
Definitions of blank assessment fields

Year 2000 Compliance

Y = Yes, it is Year 2000 compliant
N = No, it is not Year 2000 compliant
N/A = Year 2000 compliance is not a factor with this item

Classification

1 = failure could result in human death or injury
2 = failure could be disastrous to your operating unit, UIHC, or the University of Iowa
3 = failure could have substantial impact on your operating unit, UIHC, or the University of Iowa
4 = failure could result in trivial costs or only inconveniences.

Equipment Type

CH = Computer Hardware
CS = Computer Software
IE = Instructional Equipment
ST = Scientific and Technical Instruments
ME = Medical Equipment and Instruments
CO = Communications and Office Equipment
BM = Building Mechanicals
TS = Transportation Systems
OT = Other

Manufacturer

Manufacturer of item being reviewed. In most cases, it may be preferable to contact the manufacturer rather than the vendor or distributor.

Source of Compliance Information

Indicate authority you contacted to obtain the verification of Year 2000 compliance status. You may wish to include a contact name, phone number, address, date contacted, etc.

UI Departmental Contact

Name, title and phone number of individual within the department who verified Year 2000 compliance data.

Required Corrective Action

Description of action necessary to remedy Year 2000 compliance error if applicable. Examples include, software update, refitting of certain hardware components.

Estimated Cost to Correct

Best estimate of cost, if any, necessary to correct the Year 2000 compliance deficiency. Might include amount for upgrade in software to full replacement of item if no other remedy is available.

Source of Funds for Correction: Identify the anticipated source of funds to correct the deficiency. For example, it might be vendor provided, current year budget, capital budget request.

Date Product will be Compliant: Anticipated date Year 2000 remedy will be operational.

Comments: Any data pertinent to the user, departmental management, etc.

Memo 1

Appendix G
Sample Vendor/Manufacturer Memoranda

Sample memoranda and accompanying documents are provided on the following pages. The memos may be tailored to your needs and printed on University letterhead from your department.

Memo 1 might be used for the compliance review of equipment for which you need specific information relating to the storing of date components or to the testing of the device. It must be accompanied by a list of products for which you are requesting this detailed information. Memo 2 might be sent when you have a list of items for which you are requesting compliance information. It must be accompanied by the "Important Notice to All Vendors" compliance check list. You should describe one item per page, noting the product specifics in the first box. You must also send a blank check list for any products which the vendor has record of selling to you but which you did not specifically identify.

THE UNIVERSITY OF IOWA

<the date>

Chief Executive Officer
ABC Corporation
1234 Maple Street
Alltowns, Allstates

RE: Equipment operational problems due to year 2000 date change

The University of Iowa is writing about possible effects that the year 2000 date change will have on the devices that you market. Please answer the following questions in writing for each device and model number listed on the attached list and return your comments to us by *<date>*.

- Is the device(s) - including all its installed features and options - year 2000 compliant? That is, will it do the following:
  - Handle dates in the range of 1/1/1900 through12/31/2099?
  - Function in exactly the same manner before and after January 1, 2000?
  - Correctly recognize the year 2000 as a leap year?
- If the answer is yes:
  - What is the data format being used to ensure proper operation (e.g., full four-digit year, century bit only?)
  - Specifically, what test methods were used to guarantee year 2000 compliance, and what were the results of those tests?
- If the answer is no, we expect full cooperation in solving your product's year 2000 problems and require a written response to the following:
  - Specifically, what functions or capabilities are affected by the year 2000 date change?
  - Do you plan to make the device compliant? ïWhen will this compliance correction be available?
  - If you do not plan to make the device compliant, what are your plans to support the product?
  - Confirm that you will pay for the repair.
- Do you know if this device will be able to interact properly with any other device it may be connected to when the year 2000 date change occurs?

Please have an executive officer respond to these questions by the date listed above. The response must include the signature, printed name, title, address and phone number of the officer. If we do not receive a response by that date, we will assume your product is not year 2000 compliant, will begin contacting other suppliers for a replacement, and will seriously consider refraining from purchasing your products in the future.

Sincerely,

Memo 2

THE UNIVERSITY OF IOWA

<the date>

Chief Executive Officer
ABC Corporation
1234 Maple Street
Alltowns, Allstates

RE: Equipment operational problems due to year 2000 date change

A critical component of the University of Iowa's year 2000 compliance program is to insure that all University equipment will meet the year 2000 criteria and continue to function without interruption before, on and after January 1, 2000.

The enclosed forms identify one or more products purchased from you that we believe to be time and/or date sensitive in their operation, performance, and functionality and which may be negatively impacted by the century date change. It is critical that you complete these forms, providing one form for each different product, and return them to the attention of <department/unit director> no later than 30 days from the date of this letter. If the University has purchased other products from you which are not identified on the attached forms, please complete a blank form for any such product.

If you fail to complete this form(s), the University of Iowa may in its sole discretion decline to purchase products from you in the future or if your contract with the University is ongoing, the University of Iowa may begin proceedings to terminate the contract with you.

If you have questions, please call <your name and phone number>.

Sincerely,

Vendor checklist

VENDOR NAME PRODUCT:

UNIVERSITY OF IOWA - IMPORTANT NOTICE TO ALL VENDORS

The University of Iowa declares that a YEAR 2000 COMPLIANCE issue exists, or is reasonably believed to exist, with respect to the product listed above that was purchased from you. The University believes that your product is time and/or date sensitive in its operation, performance, and functionality which may be negatively impacted by the century date change (from before, on or after December 31,1999, to on and after January 1, 2000). You must complete and return this form within 30 days. If more than one product is identified, **complete each form for each product.** Also, a blank form has been provided to record other products purchased from you which are not identified above. **IF YOU FAIL TO COMPLETE THIS FORM**, the University may, in its sole discretion:

1) Decline to purchase products from you in the future; and,

2) If your contract with the University is ongoing, the University may begin proceedings to terminate the contract with you.Year 2000

Year 2000 Compliance means:

The product(s), when used in accordance with its specifications and documentation, shall:

1) Identify and process date and time data without causing any processing interruptions, abnormal terminations, or changes in performance level, characteristics, or functionality of the product(s); and

2) Identify, process and manipulate all date and time data related functions correctly (including leap year calculations, day-in-year calculations, day-of-the-week calculations, and week-of-the-year calculations); and

3) Correctly handle date and time related data, before, on, and after January 1, 2000, including but not limited to accepting input, providing date data output (if applicable), and performing ongoing operations on dates and portions of dates, including but not limited to calculating, comparing and sequencing of dates (in both forward and backward operations spanning century boundaries); and

4) Correctly store and provide output of all date and time data in a manner that is unambiguous as to century.

PLACE A CHECK MARK IN EACH OF THE BOXES BELOW THAT APPLY TO YOUR PRODUCT. PLEASE READ THE STATEMENTS BELOW CAREFULLY. DO NOT CHECK STATEMENTS THAT CONFLICT WITH ONE ANOTHER. THE BURDEN OF DETERMINING WHICH STATEMENTS APPLY TO YOUR PRODUCT IS ON YOU!!

❑ 1) The product identified herein is Year 2000 Compliant and will function as specified from the date of purchase and after without interruption attributable in whole or in part to a Year 2000 Compliance error or deficiency.

❑ 2) The product identified herein is **NOT** Year 2000 Compliant but will be made Year 2000 Compliant no later than: _____.

The Vendor will provide the following solution(s) or remedies to insure Year 2000 Compliance by the date specified above. Please explain:

_____

_____

_____

❑ 3) The product is warranted (by the manufacturer or by the seller) to be Year 2000 Compliant. The warranty is attached to this form. *(If you check this box, you must attach the warranty.)*

❑ 4) The functioning, characteristics, and performance of the product are not affected by date or time sensitivity and the functioning, characteristics, and performance of the product will not be impacted by a century date change.

❑ 5) The product is **NOT** Year 2000 Compliant and will not be made to be compliant.

❑ 6) Other options are available to make the product Year 2000 Compliant (for example: maintenance agreements, upgrades, other). *(If you check this box, you must attach the warranty.)*

_____

(Signature of Vendor's Authorized Representative/Date)

_____

(Print Name of Vendor's Representative and Title)

_____

_____

(Print Address)

_____

(Print Phone and Fax Numbers)

RETURN THIS FORM TO:

Team 2000 University-wide MONTHLY REPORT

Date: _____

		Computer Hardware	Computer Software	Instructional Equipment	Scientific & Technical Instruments	Medical Equipment & Instruments	Communications & Office Equipment	Building Mechanicals	Transportation Systems	Other
Life-Threatening Items	Identification & Assessment (% complete)									
	Resolution (% complete)									
	Projected costs to correct									
Mission Critical Items	Identification & Assessment (% complete)									
	Resolution (% complete)									
	Projected costs to correct									
Priority Items	Identification & Assessment (% complete)									
	Resolution (% complete)									
	Projected costs to Correct									
Non-Priority	Identification & Items Assessment (% complete)									
	Resolution (% complete)									
	Projected costs to Correct									
Total	Identification & Assessment (% complete)									
	Resolution (% complete)									
	Projected costs to Correct									

COMMENTS:

Section 7

Personal Computer (PC) Testing Instructions

One aspect of Y2K readiness involves ensuring the desktop computer continues to function properly after January 1, 2000. A key element of this is the PC's Basic Input/Output system (BIOS). In this section you will find:

- Instructions for performing three manual Y2K BIOS tests including one for leap year.
- Seven Web sites which offer free downloadable software that can automatically test the PC BIOS.
- A Web site which lists PC models and the Y2K disposition of their BIOS.

Personal Computer (PC) Testing Instructions

One potential Y2K problem could arise as a result of a non-compliant BIOS (Basic Input/Output System) inside personal computers. (Note: This is not an issue with Macintosh computers). Personal computers have an internal clock that is year sensitive. Some may not recognize the new century, which could cause problems with operations that rely upon the PC's clock for date information.

There are several ways to test the BIOS for compliance including manual methods, vendor databases, and free software tools. (Note: these tests ONLY test the BIOS and DO NOT test the operating system, e.g. Microsoft Windows, or any software you may be running on your PC, e.g. Microsoft Access.) No single test or utility can guarantee that a user will get through the change to 1/1/2000 without problems. Therefore, a user may wish to use several test tools. If these tests fail you may wish to upgrade the BIOS, with a software update available from the manufacturer (available for most Pentium and newer PCs), replace the BIOS chip, install a software patch that may be able to modify the date the OS reads from the BIOS, or replace the PC.

Below are some manual tests you can perform.

Manual Test 1

1. With the personal computer turned off, insert boot disk into disk drive and turn on personal computer *
2. At the DOS prompt type "date=12/31/1999" <press enter>
3. At the next DOS prompt type "time=23:58:00" <press enter>

3a. Turn off the computer, but keep boot disk in the disk drive.

4. Wait at least 3 minutes then Turn on the computer.

4a. At the DOS prompt type "date" <press enter>

5. Date should now display Current Date is Sat 01-01-2000
6. Remove the boot disk from the disk drive.

Manual Test 2

1. At DOS prompt type "Date=01/01/2000" <press enter>
2. Type "Date" <press enter> date should now display Current Date is Sat 01-01-2000

Manual Test 3 for leap year processing

1. At DOS prompt type Date 02/29/2000 <press enter>
2. Type "Date" <press enter> Date should now display Current Date is Tue 02-29-2000.

BE SURE TO RESET THE DATE AND TIME ONCE THE TEST IS COMPLETE.

Automatic Tests

There are several free automatic PC BIOS test tools available as well. The Department does not recommend or endorse any specific commercial product. The Department of Education disclaims any explicit or implied warranty as to the effectiveness or suitability for your specific needs of the test software available at the web sites below. Please carefully read the instructions and disclaimers that accompany each test tool.

Free Y2K PC test software tools can be found at the following Internet addresses:

http//www.mitre.org/technology/cots/patch.html

http://www.rightime.com/

http://www.zdnet.com/pcmag/special/y2k/index.html

http://www.onmark.viasoft.com/fix/

http://www.firmware.com/

http://www.survive-2000.com/

http://www.y2kpatch.com/

This site has links to some additional tests, including one specifically addressing problems experienced with older machines called the Crouch-Echlin Effect **http://tyler.net/tyr7020/y2kinput.htm**. MITRE is a non-profit organization that has a list of most PC models and the profiles of their BIOS including whether it is Y2K compliant. This can be found at **http://www.mitre.org/technology/cots/compliant_BIOS.html.**

**To create a boot disk follow these instructions:*

- *From the <Start> menu, choose <help>*
- *In the HELP index window, type "boot" without the quotes*
- *You should now see a link to the Windows help page on 'creating a boot disk'.*
- *By clicking the little arrow button in the Help window you will be walked through the process of creating a "startup disk"*

Section 8

Compliance of Vendors

In Y2K focus groups and surveys conducted by the Department of Education with postsecondary institutions, among the commonly cited obstacles facing institutions was "vendor cooperation". Within this section you will find:

- An article by attorney Andrew Butz, who describes the problem and provides an outline for getting started. He also covers contractual relationships, offers guidance on communicating with partners, and advice for cooperative plan implementation.

- Columbia University's Sample Letter to Vendors

- Columbia University's Guide to the Evaluation of Vendor Compliance Claims

- Sample language addressing Y2K that can be modified and used in future procurement

Managing the Y2K Compliance of Suppliers and Business Partners

by Andrew Butz

Even if you have made sure all of your institution's computer systems are Year 2000 compliant, you could still face unexpected problems come New Years Day 2000. Thatís because your own computers aren't the only ones your school relies on. Now is the time to ensure that all of your suppliers and business partners are Y2K compliant too.

Suppliers that may need Y2K attention include those who provide essential materials such as fuel, food, and lab, medical, and office equipment, or who maintain and repair critical equipment. Others may include partners who handle institutional funds (banks, investment firms, accountants), work with institutional data (information systems contractors, data management vendors, testing services), or team with the institution in teaching, research, and service delivery in facilities like hospitals and clinics. Don't forget organizations who provide scholarships, grants, and significant kinds of operating revenue, including government agencies and philanthropic groups.

You may even depend on organizations with which you do not even directly deal–the suppliers and partners of your suppliers and partners. You need to evaluate how much of the needed due diligence is yours directly, and how much should be expected of–and requested from–your direct suppliers.

Like your institution's internal compliance program, your external program will require planning, communication, funding, execution, and testing, all on a timely basis. It will demand ongoing communications, because you will continually need information, updates, and assurances from your suppliers.

Getting started

To manage external Y2K compliance, you will need to:

- Identify each potentially affected institutional operation and determine how much it depends on outside vendors and other business partners.
- Identify key vendors and business partners, focusing on those whose services could not easily be replaced or supplemented without significant planning or cost.
- Determine what information, assurances, testing and other evidence of Year 2000 compliance your institution needs from each business partner.
- Establish a system for tracking each part of the compliance process. Ensure that your institution's files and your business partners' files document your requests for assistance and assurances regarding Year 2000 compliance, your business partners' responses, all follow-up efforts to execute joint efforts, and any notice to business partners of events that could adversely affect your institution or its rights.

Contractual Relationships

Chances are that current or planned written contracts define the relationship between the institution and its partners. Do those contracts address Year 2000 issues either expressly or by legal implication?

If a contract addresses Year 2000 issues directly, you need to determine whether the express provisions will meet your needs. If the contract calls for not-as-yet provided information, testing, or further assurances, you should take steps to request such performance, satisfy any pre-conditions owed by your institution, and evaluate the adequacy and completeness of the delivered performance. If contracts do not address Year 2000 issues directly, but may do so by implication, you will need to determine with legal counsel's help whether the provisions meet your institution's needs, including whether and how they can be enforced.

In some contracts, such as those with expressly limited warranties and representations, your institution may lack adequate Year 2000-related assurances and remedies. If so, consider renegotiating those contracts or the portions with Y2K implications. You can renegotiate either upon renewal, when your institution will have the most bargaining power, or as part of a request for assurances that your partner will be able to perform in the Year 2000 environment.

You may conclude that a contract holds the institution itself responsible for ensuring Year 2000 compliance. Where that arrangement is appropriate, you need to determine whether your internal Y2K program can deal with potential problems, or whether you need to address the issue with some other supplier or business partner. Whenever your institution negotiates or renews a contract with its business partners, the written contract should expressly allocate Year 2000 responsibilities.

Communicating with Your Partners

Now that you are ready to contact your suppliers and business partners, what should you ask for? At a minimum, you should request specific information on your partner's Year 2000 compliance efforts and written assurances that their efforts will protect the institution's interests.

You will want to ask what the business partner is doing to achieve Year 2000 compliance, including efforts to identify critically sensitive systems and functions; find and fix, upgrade or replace non-compliant systems, programs, and equipment; and ensure that its own suppliers and service providers are also Year 2000 compliant. You also need to know who you will work with on shared efforts to achieve and test for actual year 2000 compliance.If your business

partner cannot or will not provide specific information right away, your request should indicate that you need to know when information will be available. If information is in fact unavailable, your request should indicate that you need express assurances that the partner will accept responsibility for losses resulting from its failure to provide goods and services or fulfill other responsibilities because the partner failed to institute and execute an appropriate Y2K compliance program.

If your partner hesitates to cooperate or provide specific information, or evades questions about contractual assurances, consider whether your institution should continue relying on that partner. At the very least, you will need to line up potential alternative partners who can demonstrate Year 2000 compliance.

Implementing the Plan

Initial contacts might indicate that your partner is not fully Y2K compliant but is prepared to work with you in good faith. In that case, you can begin working out the steps you believe will satisfy your institution's need for sufficient information, cooperation, and comfort.

That means briefing your partner's representatives on your own Y2K program so they can understand your compliance needs. This will help them pull together the necessary resources. This is particularly important in cases in which you will need to actually test systems to demonstrate compliance.

In some cases, it may be appropriate for you to provide Y2K help to your partner. Your assistance in working with your partner's partners may be an important step in ensuring the level of compliance your institution needs.

After implementing your external Year 2000 compliance program, be sure to keep internal decision makers informed about progress and setbacks. This will help the institution deal with the inevitable spate of failures, deficiencies, or other unpleasant surprises that may occur despite your best efforts.

In sum, you should take steps to determine if your current partners are Y2K compliant. You may have to be prepared to lessen your reliance on noncompliant and uncooperative partners, find alternative suppliers who are Y2K compliant, demand adequate disclosures and contractual assurance as part of each new contracting event, monitor your institution's partners for actual compliance, and (last but not least) document your own institution's due diligence in preparing to meet the Year 2000 problem.

Andrew Butz is Of Counsel at Gilberg & Kiernan, UE Select Counsel in Washington, D.C. *Reprinted with permission of United Educators Insurance Risk Retention Group, Inc., Education's Own Insurance Company, and UIMC, a management company serving education, copyright UIMC. "Risk & Reason" Fall 1998, Volume 6, Number 2. All rights reserved.*

Vendor Evaluation -Sample Letter to Vendors

Compliance Tool Kit for
Columbia University Departments
http://www.ais.columbia.edu/ais/html/sample_letter.html

Departmental Address

Date
Software Company
Address
City, ST, zip

Dear Sirs:

We are reviewing all our computing applications to determine readiness for processing in the Year 2000 and beyond. We have identified the following hardware and/or software products as being purchased or licensed from you, written by you or maintained by you. For each product, please provide the following information:

Is the product Year 2000 compliant?

Yes, compliant now [ ] Will be made compliant [ ] Cannot be made compliant [ ]

If the product is now Year 2000 compliant, please provide a written statement of what Year 2000 compliance means, and how it may be demonstrated. Please indicate the earliest version or model number and/or earliest release date of the compliant product.

If the product is to be made compliant, please provide a written statement of your plans for achieving compliance and your target dates for release.

Your cooperation and prompt response will be greatly appreciated.

Sincerely,

Jane Doe
Year 2000 Coordinator

[Insert list of hardware/software products from the vendor, showing current model, version or release numbers, where appropriate]

Compliance Tool Kit for Columbia University Departments
http://www.ais.columbia.edu/ais/html/guide_to_eval.html

Guide to Evaluation of Vendor Compliance Claims

Many hardware and software vendors are now providing Year 2000 compliance information for their products on their WWW sites. You may also receive written statements from some vendors or request year 2000 statements from them. But what does it mean if a vendor claims: "This product is Year 2000 compliant," or "All our products are ready for the Year 2000"?

Year 2000 compliance may mean several things:

- The product does not store dates or process information using dates, and therefore will not be affected by the century rollover.
- The product does store dates or process by date, but year fields are all 4-digit, so 20th and 21st century dates will be recognized and handled properly.
- Internal (and perhaps input or output) year fields are 2-digit, but the computer translates years into 20th or 21st century dates based on a 'window' or cutoff year. (For example, years 00-40 will be assumed to be 2000-2040, and years 41-99 will be assumed to be 1941-1999.)
- Dates, including years, are calculated from some starting point (as in most UNIX processors) and will be valid until sometime later in the 21st century or beyond.

Make sure you know which the vendor means, as it may have implications for the use of the product in specific circumstances or for interfaces with other systems.

Hardware products, operating system software, and application program software change and are upgraded over time. Determine from the vendor what specific model or version of the product is asserted to be Year 2000 compliant, as of what date. Compare that to the model or version you are running and upgrade if necessary.

If the product in question is not yet Year 2000 compliant, but the vendor says that it will be, determine how the vendor plans to achieve Year 2000 compliance and when.

Determine or ask if and how use of the product will change because of year 2000 changes. If dates have always been entered in the format mm/dd/yy, will they now have to be entered as mm/dd/yyyy? Will existing spreadsheets, report templates, or older files have to be altered or expanded to accommodate the new version?

Whenever possible, test all products, in the actual environment in which you use the product. Do not accept vendor claims or statements at face value. Even if the product has been converted to handle dates past December 31, 1999, there may be unexpected results in any given specific environment.

Contract and Procurement Language

To ensure that information technology purchased by a school is Y2K compliant, the school may include a clause similar to the following in its contracts. The school may also wish to include other more specific requirements. E.g, the school may wish to require a specific date format needed to interact with its computer systems, to require that the items purchased meet specified tests for Y2K compliance or to provide for a longer than normal testing period. If a buyer specifies a particular brand name and model, then the buying agency is responsible for Y2K compliance, unless the item was designed by the contractor or its affiliate. Thus, the following clause presumes that a school will not specify a brand name and model unless the school has already determined that the item being purchased is Y2K compliant.

Sample Clause:

DELIVERY OF YEAR 2000 COMPLIANT INFORMATION TECHNOLOGY

(a) Each hardware, software or firmware product delivered under this contract must be able to process accurately date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations to the extent that other information technology, used in combination with the information technology being acquired, properly exchanges date/time data with it.

(b) If the contract requires that specific hardware, software or firmware products must perform as a system, then the requirements of paragraph (a) of this clause shall apply to those products as a system.

(c) The requirements of paragraph (a) of this clause do not apply to products specified by the [name of school or agency awarding the contract] on a "brand name and model" basis, unless the product was designed or produced by the contractor or one of its affiliates.

Section 9

Contingency Planning

Assuring that critical business functions continue in the event of a Year 2000 related system failure is critical to the goal of educating students, including providing financial assistance to needy students. Contingency planning is the process of identifying critical business functions and planning alternative procedures to assure that critical business functions continue uninterrupted while system failures are repaired. Within this section, you will find:

- An article by B.L. Bruner that describes the importance of contingency planning and summarizes the process.
- *Contingency Planning Best Practice*, an article that provides more details about the process of contingency planning and includes a template that can be used in the development of plans.
- Sample University Y2K Contingency Planning Process Project.

Contingency Planning Can Lessen the Impact of Inevitable Y2K Failures

by B.L. Bruner

No matter how carefully your institution prepares for Year 2000 problems, some systems will still fail because of external factors over which you have absolutely no control. That makes contingency planning an essential component of your Y2K strategy.

The direct costs of Y2K failures will be substantial, but they may pale in comparison to the indirect costs ranging from adverse publicity to litigation these failures will bring. In today's litigious environment, many will seek to hold institutional administrators and their agents legally and managerially accountable for both internal failures and the internal consequences of external failures.

You can avoid many of those consequences by planning solutions for Y2K failures that could affect personal safety and security, cause substantial costs or lost revenue, damage the institution's public image, or expose it to litigation risk. Your plan needs to go beyond the direct, operational impacts of the Y2K problem and address consequential actions and conditions as well. For example, it will take money and staff time to address the work-around solutions and infrastructure damage that the Year 2000 problem will cause.

What is Contingency Planning?

Y2K contingency planning is a process that runs parallel to, and in concert with, your overall remediation and compliance effort. It is the process of anticipating how and when systems may fail or be disrupted, and crafting alternative approaches to minimize those possibilities. Contingency planning is not an eleventh-hour strategy that you can begin developing after dealing with the nuts and bolts of Y2K compliance. The two must happen simultaneously.

Be prepared to develop several alternatives for activities that may be disrupted by Y2K problems. Depending upon the circumstances, you may need to consider not just how you will carry out institutional functions, but also what the legitimate objectives of those operational functions might be. Among your choices: continue normal operations, sustain operations in a degraded mode, take a temporary hiatus, or completely rethink how to achieve the overall operational goal. Practically speaking, these options might be as drastic as substituting fully manual procedures for computer functions or even postponing the start of the 2000 spring semester.

Contingency Planning Step by Step

If you are starting the contingency planning process now, recognize that you've got some catching up to do. You'll need to move quickly and deliberately. First, conduct a risk assessment of your institution's mission-critical processes (both business and academic) and high risk activities (personal safety and security, threats of litigation, etc.). The risk assessment is the basis for setting priorities and defining the contingency planning framework and scope.

Remember, at the contingency planning stage, you are assessing processes and activities, not computer system risks. Your school may face significant risks unless you identify and address all critical processes. For each selected mission-critical process and high-risk activity, follow these steps:

- Involve a cross section of functional and technical personnel in the effort. For example, a contingency plan for maintaining dorm security might involve staff from housing, student affairs, facilities management, and campus police.
- Set concrete contingency objectives for each process for example, continue normal operations, continue in limited mode, outsource, temporarily suspend operations, or cease operations altogether. Simplify objectives wherever possible.
- Assign responsibility and authority for developing the alternatives (including business and academic policy-and-procedure changes where required). It will often prove more expedient to rethink processes from scratch rather than building on existing processes.
- Quantify the resource requirements for the alternative, including staffing, materials, supplies, facilities, hardware, software, communications, services, and controls.
- Document, document, and document your alternatives and your contingency planning processes. This is your evidence of due diligence.
- Establish criteria for implementing each alternative. Trigger points might include such scenarios as falling behind on remediation efforts or computer-related failures such as service interruptions, security breaches, systems shut-downs, or data corruption.
- Design and conduct a testing or trial regimen that simulates reality.
- Develop training and communications to help people understand the alternatives. Put them into effect as soon as possible. Publicize procedures for implementing each plan and its alternatives. Donít let any action surprise anyone.
- Establish up-front criteria and procedures for returning to normal operating mode.
- Identify necessary post-contingency procedures for recovering lost, damaged, or reformatted data.
- Regularly revisit assumptions and progress. Successful risk avoidance is a dynamic process.
- Get outside review and assistance to ensure that you have exercised full due diligence.

Remember, you will need to follow each of these steps for every mission-critical process and high-risk activity you identify.

There will be winners and losers in the Year 2000 effort. The real winners will be those who do not just avoid major problems, but who use this opportunity to reexamine service levels and service delivery. The winners will see contingency planning as a strategic investment in improving the institution's image, competitive advantage, and efficiency. The clock is ticking now. Get started.

B.L. Bruner is vice-president of the Kaludis Consulting Group, an executive consulting and management services firm specializing in support to higher education. Reprinted with permission of United Educators Insurance Risk Retention Group, Inc., Education's Own Insurance Company, and UIMC, a management company serving education, copyright UIMC. "Risk & Reason" Fall 1998, Volume 6, Number 2. All rights reserved.

State of MinnesotaYear 2000 Project
www.state.mn.us/ebranch/admin/ipo/2000/contbest.html

Contingency Planning Best Practice

Purpose

This document was designed to assist State Agencies with Year 2000 projects by providing direction and recommendations for establishing contingency plans.

Background

Definition

A contingency plan describes how an agency intends to respond to events which disrupt normal operations of an information resource. The plan provides a road map of predetermined actions which will:

- Reduce decision-making during recovery operations
- Resume critical services quickly
- Enable resumption of an acceptable level of service at the earliest possible time in the most cost-effective manner

Good planning reduces the number and magnitude of decisions which must be made during the period when exposure to error is at a peak. Disruptions covered by a contingency plan may be minor or may include instances where normal government functions cannot be performed for an extended period of time.

Objectives

An important factor with any contingency plan is its objective. All contingency plans do not have the same goal. For example, it may be cost-prohibitive to provide normal levels of response and service during contingency mode, so an alternative level may be the target of the contingency plan. There is no correct answer for all agencies ñ agency business priorities will determine the objective of the plan.

Below are some forms that a contingency plan can take:

1. Normal level of service – providing a level of service equal to the level provided during normal service. An example of this form of contingency plan is a plan for a personal computer that specifies replacement with a spare machine of equal power.

2. Degraded service – providing a level of service that is less than the level provided during normal service. An example of this form of contingency plan is a plan for an accounts payable system which normally pays bills within five days of receipt. The contingency plan calls for hiring two temporary staff to process invoices within 10 days of receipt.

3. Simplified service – providing a different level of service than the level provided during normal service. An example of this form of contingency plan is a plan that was suggested for the U.S. Internal Revenue Service – convert to a simple, flat tax policy until the IRS information systems are made Year 2000 compliant.

4. No service – ceasing the service. This may be an option for a limited number of agency information resources.

Levels

Contingency plans may also have different levels. That is, different contingency actions would be in effect based upon certain characteristics of the failure. For example, a contingency plan may specify a degraded, manual process for the first 30 days of a failure, and convert to a simplified process for any period of time over 30 days. Levels of a plan will be based upon the agency's business priorities.

Complexity

The level of complexity of a plan should be appropriate for the information resource that it is intended to protect. For example, the contingency plan for a fax machine that fails could be to simply call service or purchase a new one. However, it is important that all contingency plans be clearly documented to aid the decision-making process in the case of a failure.

The need for plans

Information Resource Scope

For most agencies, information resources are not a luxury for delivering services to citizens. These resources support business processes, resulting in desired outcomes crucial to the agency's mission. This is why the Year 2000 issue is so critical — if the State is unable to plow roads, pay benefits to citizens, or manage natural resources, there is a business problem, not a technology issue. Citizens will not ask what piece of hardware or software is broken, they will ask why there has been an interruption in an expected outcome. As the diagram below illustrates, desired (and in some cases, statutory) outcomes will be placed at risk if information resources fail.

The Likelihood of Failures and the Importance of Planning

Although most agencies are working to correct Year 2000 problems, it is inevitable that some things will be overlooked, ignored, or not completed on time. This is particularly a concern due to the large number of information resources owned by the State. Another certainty is that there are things outside of the State's control that could affect agencies in the Year 2000. One way to be adequately prepared is to develop contingency plans to address potential failures.

Contingency plans are necessary for any organization, as shown by the examples below:

- Many businesses that were destroyed by the Federal Government building bombing in Oklahoma City and in the World Trade Center bombing in New York City never reopened because they were unable to recover from the destruction of property and records.
- The UPS Strike of 1997 affected organizations to varying degrees. Some firms that were heavily dependent on UPS made plans before the strike to use other carriers. As a result, these firms were able to maintain their level of customer service. Conversely, some organizations that did not plan saw shipping times increase up to 300%.
- A State agency has already invoked a contingency plan on a project to replace a mission critical system. The project is behind schedule, so the agency is going to fix the existing system in case the new system is not ready for implementation in time to avoid Year 2000 problems. Relation to other types of plans

Relation to Other Types of Plans

Contingency plans are related to, but do not take the place of, other types of plans. These other plans are listed below:

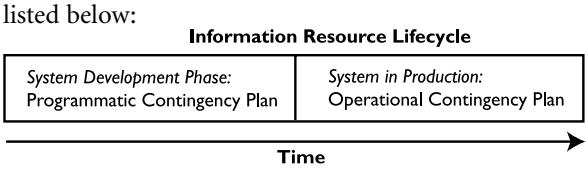
Risk Management Plan/Strategy
A Risk Management Plan identifies risks facing an agency and abatements to address these risks. Contingency plans for information resources are one component of an agency's risk strategy, and thus should be consistent with the philosophy and goals of the overall risk plan. However, contingency plans for information resources are narrower in scope, dealing only with information resources. An agency risk strategy is broader in scope, including abatements for risks in all resource categories such as staff, facilities, etc.

Disaster Recovery Plan
A Disaster Recovery Plan covers procedures for resuming agency functions in the case of a catastrophe. This type of planning assumes that few or none of the agency's normal operations can function. Contingency planning is similar to disaster planning, with two major differences. First, contingency planning doesn't assume the source of the failure, only the steps needed to resume normal operations. Secondly, contingency plans do not preclude the use of agency resources (e.g., facilities) that may not be available in the case of a true disaster.

Backout Plans
Backout (also known as Rollback) plans are specified during the implementation phase of a systems development project. These plans describe procedures to back the new system out of production in the case of problems. The nature of backout plans is short-term – they only are an option for a short time. After some period of time, it becomes impractical to revert back to the old production system. Conversely, a contingency plan is longer term – it only needs to be changed if the underlying assumptions upon which the plan was built change. It is best to think of a backout plan as a contingency plan to handle a specific failure – that is, the failure of a newly implemented system to perform as expected.

Types of Contingency Plans

The State has defined two types of contingency plans which are listed below:



1. Programmatic
Also called Triage, Programmatic Contingency Plans refer to planning which covers the Development phase of a system implementation project. It focuses on actions to be taken when it appears that a system development project will not be completed in time to avoid Year 2000 problems. The need for programmatic contingency goes away when a system is put into production. An example of this sort of contingency would occur when some previously overlooked programming code has Year 2000 problems, and not enough time is left to fully fix all of the problems.

2. Operational
Operational Contingency Plans cover information resources that are already in production. It focuses on the resumption of functions performed by a resource that has failed. For example, this sort of contingency would be implemented if a payroll system experienced a failure.

For more detailed information on Programmatic and Operational Contingency Plans, visit this website: **www.mitre.org/research/y2k/docs/CONTINGENCY_GUIDLELINES.html**, or contact the Minnesota Year 2000 Project Office.

Information Resources Which Require Contingency Planning

Agency Risk Management Plans and business priorities will determine the need for contingency plans. All information resources are candidates for plans, including:

- Custom Applications
- Hardware
- Package Software

In addition, other candidates for plans include:

- Interfaces
- Firmware
- Business Partners and Service Providers
- Areas regulated by government

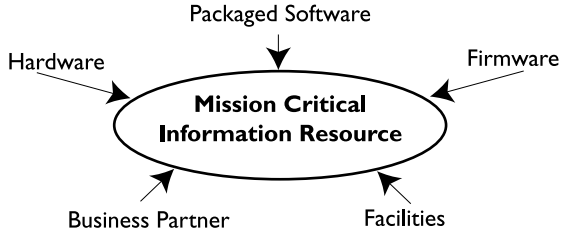
At a minimum, the Minnesota Year 2000 Project Office recommends the following:

- Agencies should create Programmatic contingency plans for all mission critical information resources that are under development:
  - to fix Year 2000 issues,
  - to replace information resources with Year 2000 issues, or
  - for any other reason.

Agencies should create Operational contingency plans for all mission critical information resources.

Related Information Resources

Deciding which resources need contingency plans is not always a straightforward exercise. Information resources are highly integrated, and as a result, a mission critical resource may depend upon a supposedly non-mission critical resource. This must be factored into the decision of which information resources require contingency plans, as illustrated below:



The depth of related information resources that require plans is a prioritization issue which must be determined by each agency.

Elements of a successful plan

Objective of the plan
As discussed above, all contingency plans do not have the same objective. For example, the plan could have any one of the following objectives: continue normal operations, continue in a degraded service mode, exit the function as quickly and safely as possible, etc. The objective of the plan will be determined by the business priorities of the agency, and by the complexity and cost of alternative contingency strategies.

Criteria for invoking the plan
There should be clear, definitive, and automatic criteria for invoking the plan. (These are sometimes referred to as "escalation" criteria.) Limiting the amount of subjectivity in these criteria will facilitate swift actions to address any failures. Examples of clear criteria for a programmatic contingency plan include a missed renovation milestone or the departure of a predetermined number of key staff. Examples of clear criteria for an operational contingency plan include a predefined number of system failures or a predetermined length of downtime.

Expected life of the plan
The plan should define the length of time that the information resource can continue operating in contingency mode. If there are multiple levels to a plan, it should define the length of time that the plan can remain in each level.

Roles, responsibilities, and authority
Identifying roles, responsibilities, and authority is important, because in contingency mode they may be different compared to normal operating mode.

Procedures for invoking contingency mode
The steps for implementing contingency mode should be clearly listed.

Procedures for operating in contingency mode
The steps for running in contingency mode should be clearly listed.

Resource plan for operating in contingency mode
As with roles and responsibilities, the use of resources in contingency mode is often different from normal operating mode. Examples of resources which may be managed differently include staff, schedule, materials, supplies, facilities, hardware, software, and communications equipment.

Criteria for returning to normal operating mode
There should be clear, definitive, and automatic criteria for exiting contingency mode. Limiting the amount of subjectivity in these criteria will facilitate a smooth transition back to normal operating mode. Examples of clear criteria for returning to operating mode include completion of a test run of transactions and approval from users and management to return the information resource to production.

Procedures for returning to normal operating mode
The steps for exiting contingency mode should be clearly listed.

Procedures for recovering lost or damaged data
Often the conditions that led to a failure result in damaged or lost data. In addition, during contingency mode, data may not have been entered into the system. Procedures must be established to ensure the data integrity of the system, which may include entering in all data that was missed or corrupted during the failure.

Estimated cost of the plan
Costs must be estimated in a contingency plan so that if the plan is invoked the agency will have an idea of the funds required.

Post contingency plan
There should be a provision for a debriefing after the plan has been executed. Any problems or improvements should be noted and changed in the plan. Any major changes should be approved by users and management.

Steps to achieve a plan

Agency-Wide Activities
The following steps should be performed at an agency-wide level:

Obtain business user and management support for contingency planning.
The planning process has little chance of success without buy-in from these groups. Obtaining this support may require educating agency personnel about the need for plans.

Review the agency's mission, strategic plan, and risk management plan.
These documents may include information such as service levels and response time which will guide the contingency planning process.

Determine the information resources that will require contingency plans.
This will be dictated by an agency's business priorities, which should balance the cost of creating plans with the risk of an information resource failure. For most agencies, this will include, at a minimum, all mission critical resources.

Identify the type of plan needed for each of these information resources.
Specifically, determine whether a Programmatic plan, an Operational plan, or both types of plans are required.

Determine the need for plans for related information resources.
For example, if it is determined that a software application needs a plan, the hardware for this application may also need a plan.

Prioritize the plans that will be created.
Begin work on the highest priority plans first.

For each information resource

The following steps should be performed for each information resource that requires a contingency plan:

Determine points of failure.
This is an identification of components which could fail. This could include components of the information resource, or it could include related information resources. For example, points of failure for a software application could include a program module within the application, the hardware which runs the application, the operating system which runs the hardware, or communication lines which feed data to the application from other locations.

Determine risk and impact for each point of failure.
This is an estimation of the likelihood and consequences of the potential failure.

Develop a contingency plan to deal with each point of failure.
Build the plan to address the potential failure, using the contents in the *Elements of a Successful Plan* section. A single contingency plan may deal with multiple points of failure, particularly if the points of failure are closely related.

Test the plans (as appropriate).
As with any significant effort, testing is critical to ensure the plan will work as anticipated. Testing of contingency plans may be expensive and impractical, so agency business priorities should determine the degree of testing which makes sense. However, practical experience has proven that a tested plan has a greater chance of success than an untested plan.

Obtain management sign-off for each plan.
This is a crucial last step to the process of building a plan. It is likely that management will not be actively involved in the creation of the plan. Therefore, management must understand and approve each plan. This is important because many plans have unavoidably high costs. For example, the contingency plan for failure of a particular system may be to hire 30 temporary employees to process data at a level of 50 percent degradation in speed and accuracy from the production system. Management must understand the gravity and scope of alternative solutions in order to properly allocate resources.

Resources and Further Reading

- General Services Administration:
  www.gsa.gov/gsacio/bpimpph.htm#contin
- MicroSoft Press, Steve McConnell: Rapid Development
- MITRE:
  www.mitre.org/research/y2k/docs/CONTINGENCY_GUIDLELINES.html
- Project Management Institute:
  A Guide to the Project Management Body of Knowledge
- State of Texas:
  www.dir.state.tx.us/oops/stgyplan/index.html
- Year 2000.com:
  www.year2000.com/archive/NFtudor.html
- Year 2000 Journal: 1997, Volume 3
- The Federal Financial Institutions Examination Council's "Guidance Concerning Contingency Planning in Connection with Year 2000 Readiness"
  http://www.ffiec.gov/y2k/contplan.htm

State of Minnesota Year 2000 Project
Contingency Planning Template
June 1998

Information Resource

Type of Plan (Programmatic or Operational)

Agency _____

Date _____

Created By _____

Related to Other Information Resources/Contingency Plans? (if yes, list below)

Agency Head Approval _____

Date _____

Objective of the plan

Criteria for invoking the plan

Expected life of the plan

Roles, responsibilities, and authority

Procedures for invoking contingency mode

Procedures for operating in contingency mode

Resource plan for operating in contingency mode

Criteria for returning to normal operating mode

Procedures for returning to normal operating mode

Procedures for recovering lost or damaged data

Estimated cost of the plan

Post contingency plan

Sample University Y2K Contingency Planning Process Project

(Follows GAO guidelines)

Phase I: Project Initiation

1. Obtain Senior Administration (Pres/VP) level support.
2. Select Contingency Planning Core Staff to provide overall leadership and support. (Ex: Sr. management SFA, BO, and Registrar staff)
3. Identify Critical Business Processes. (Ex: determine eligibility and award students, disburse funds to students, enroll students, payroll , etc.)
4. Select Business Process Contingency Planning (CP) Team Chairs to lead the analysis, planning, and testing activities for each of the critical business processes. (Ex: assistant/associate director level in the business process principal office)
5. Select team members for each critical business process CP Team (consider including staff knowledgeable in all areas of the business process and systems staff and consider manager and operational levels of staff).
6. Develop project plan schedules for each critical business process.

Phase II: Business Impact Analysis

1. Describe all critical business processes, including all business process elements, data systems, and data exchange relationships and all dependencies on other processes and systems including other internal (Ex: admissions, registrar, student financial aid , business offices) and any external agencies and business partners (Ex: ED, software venders, servicers, GAs, lenders).
2. Identify and document system failure scenarios. (Ex: what may fail and when will it fail such as, your system is unable to draw down funds from the Departmentís system on December XX, 1999, for winter term, 2000)

3. Perform risk analysis of each critical business process.

- Determine impacts/consequences of internal and external system failures on the performance of the business process; the probability that a failure will occur; and the likeliness of the potential failure. (Ex: what happens if the system fails such as, for winter term, 2000, your school cannot draw down funds so that students will not be able to pay their bills)
- Determine critical business process and recovery priorities. (Ex: will it matter or how significant are the consequences of the failure such as, if students cannot pay their tuition bills, they cannot enroll)
- Contact external partners (ED, software venders, servicers, guaranty agencies, lenders) about Y2K compliance status to determine if there are concerns that need to be addressed in the contingency plan.
- Review the Y2K disaster recovery/contingency plans for each system that interacts with the each of the business processes.

4. Assess and document infrastructure risks. Review the contingency plans of critical public services (power, telecommunications) and determine whether emergency alternatives are available.
5. Define minimum acceptable levels of service for each critical business process. (Ex: Students may go X days without paying their tuition bills, but need funds in Y days to buy books, pay rent, etc.)
6. Obtain feedback from customers. (Ex: students, administrators, faculty, external partners)
7. Present business impact analysis to all teams, core staff, and senior administrators.

Phase III: Contingency Planning

1. Identify potential alternative procedures (Contingency Plans) to continue business processes disrupted by data system failures. (Ex: If the school's system cannot draw down funds from the Department, the school will give emergency loans to students to buy books, pay rent, etc.) or risk mitigation scenarios to prevent a disruption in business processes. (Ex: post University scholarship funds to students' accounts in advance of December 31, 1999)
2. Assess the costs, benefits, risks, and practicality of identified alternative procedures including: levels of service that can be achieved and the time needed to acquire, test, and implement the alternate procedures.
3. Define and document trigger events that would activate contingency plans and length of time for each plan.).
4. Obtain views of affected communities concerning potential contingency plans. (Ex: students, administrators, faculty, external partners)
5. Recommend best contingency options to senior administrators and obtain approval or amend plans.
6. Obtain needed resources (funding, staff, contracts, equipment, and other resources).
7. Establish "business process resumption" teams responsible for implementing contingency plans.

Phase IV: Testing and Rehearsal

1. Develop and document contingency test plans.
2. Train test/rehearsal teams.
3. Execute tests/rehearsals of contingency plans in cooperation with affected communities. (Ex: other administrative offices and external partners)
4. Evaluate test results and adjust contingency plans as needed.
5. Validate the capability of contingency plans, insuring adequate levels of record-keeping, data security, financial integrity, and business performance.
6. Update contingency plans based on lessons learned and re-test as needed.

Section 10

Y2K Information and Resources

In this section you will find additional Internet resources, further information from the U.S. Department of Education, and a copy of the questions and answers most frequently submitted to the Department regarding Y2K. In the Y2K Internet Resources-Web sites section, you will find Web sites which provide information concerning:

- The Department of Education's Y2K Status
- Other Postsecondary Institutions' Y2K Plans
- Y2K Best Practices
- Y2K Legal Information
- Vendor Information
- Tools for Locating Y2K Consultants and Qualified Personnel
- General Y2K Articles and Information

The next document provides a list of the Dear Colleague letters that have been sent to postsecondary institutions addressing the Y2K issue.

The "Frequently Asked Questions" segment provides an updated Y2K status of the Department of Education's software releases, date standard formats, and other questions.

Y2K Internet Resources - Web Sites

U.S. Department of Education Year 2000 Project: **http://www.ed.gov/y2k** - The Department's Year 2000 site, which includes updates on ED's preparations for Y2K, Frequently Asked Questions (FAQs), best practices, and useful tools and documents for schools.

U.S. Department of Labor Year 2000 page: **http://www.dol.gov/dol/cio/public/programs/y2k/y2kgrap.htm** - Includes information about the Department of Labor's Y2K preparations and links America's Job Bank and a number of related government sites.

EDUCAUSE Year 2000 Issues: **http://www.educause.edu/issues/y2k.html** - Site provided by EDUCAUSE, the association formed by the merger of Educom and CAUSE. EDUCAUSE focuses on the management and use of computational, network, and information resources in support of higher education.

GSA Year 2000 Information Web Site: **http://www.gsa.gov/gsacio/yr1.htm** - Site provided by the General Services Administration of the federal government. Includes information on the Social Security Administration's preparations for Y2K, best practices, and recommended Y2K web sites.

Microsoft Year 2000 Resource Center: **http://www.microsoft.com/technet/topics/year2k/default.htm** - Provides white papers on Y2K issues, Frequently Asked Questions about Y2K, an online seminar on the impact of Y2K on organizations, and specific details on Y2K preparedness of Microsoft products. To find a number of very practical tools, select "Services and Tools" from the main Microsoft Y2K web page.

MITRE: **http://www.mitre.org/research/y2k/** - Very useful tools and information provided by the MITRE Corporation, a non-profit organization working with the Air Force Electronic Systems Center, and the Defense Information Systems Agency (DISA). See in particular the "COTS" (Commercial Off The Shelf) software Y2K compliance information.

NSTL: **http://www.nstl.com/html/nstl_y2k.html** - A leading provider of testing services to business and industry, including the YMARK2000 testing tool which is downloadable from this site. In addition, NSTL lists a large number of hardware vendors with their Y2K compliance status.

President's Council on Year 2000 Conversion: **http://www.y2k.gov/** - Provides index of web resources on Y2K by economic sector (including education), a toolkit for understanding the Y2K challenge, best practices, and a link to America's Job Bank for employers and job seekers.

PSU Year 2000 - Sites of Schools and Organizations: **http://www.psu.edu/Year2000/links/links.html** - College and university Y2K web sites, prepared by the Pennsylvania State University. Some sites include comprehensive Y2K plans.

Small Business Administration: **http://www.sba.gov/y2k/** - Help for small businesses and other small organizations, including a self-assessment, checklists, a toolkit, slide show, readiness worksheets, Y2K consultant database search and sample letters to suppliers.

Vendor 2000 Data Base (EDS): **http://www.vendor2000.com/** - A repository of over 129,000 (as of 9/15/98) vendors' hardware, software, and other specialized products, with their current Y2K compliance status. This site was developed and is maintained by Electronic Data Systems (EDS). To search for the Y2K status of a particular product, first select the vendor from an alphabetical listing, and then select that particular vendor's product, to determine which version is Y2K compliant.

Washington Post Year 2000 Links and Resources: **http://www.washingtonpost.com/wpsrv/washtech/longterm/y2k/links.htm** - The Washington Post's WashTech Millennium Bug Report, including links to vendors and consultants, as well as other business, federal, state and local government resources.

Windows Magazine: Year 2000 Crisis: **http://www.winmag.com/people/melgan/year2000/default.htm** - Stories, columns, freeware and shareware to help individuals and organizations deal with the "Year 2000 Crisis."

Y2K Law Site: **http://www.y2k.com/legalpage.htm** - Legal issues pertaining to Y2K, prepared and maintained by the law firm of Williams, Mullen, Christian, and Dobbins. Includes papers, seminars, legal links, and contracting pointers.

Yahoo! Year 2000 Coverage: **http://headlines.yahoo.com/Full_Coverage/Tech/Year_2000_Problem/** - Yahoo's complete coverage of the Y2K problem, with recent news stories, live net events, government Web sites, and listings of Y2K consulting companies.

Year/2000 Journal: **http://www.y2kjournal.com** - A Web magazine dedicated to the discussion of the Y2K century date problem, covering specific aspects of the millennium bug. Includes links to a number of vendor Y2K sites.

Y2K Internet Mailing List

The Higher Education Year 2000 discussion list focuses on the Y2K needs of colleges and universities, including contingency planning, vendor issues, testing, and more. To subscribe, send the message "subscribe higher-ed-y2K" (without the quotes) to the email address: **majordomo@lists.stanford.edu.**

Y2K Information from the U.S. Department of Education

The Department is relying on the Internet to distribute Y2K information. For updated information on the status of the Department's Y2K renovation work, data exchange testing information, and other outreach activities check this site regularly: **http://www.ed.gov/y2k.**

If you are interested in getting a free copy of the December 7, 1998, Year 2000 Teleconference video, please call 1-800-USA-LEARN.

This Kit may be duplicated without further permission. It can also be downloaded and printed from the Department of Education's Y2K web site: **http://www.ed.gov/y2k.**

Over the course of the past two years, the Department has issued several Dear Colleague letters that address the year 2000 issue. These letters can be found on the web site listed above.

- October 6, 1998
  Letter, advising federal grantees of their responsibility to address the Year 2000 issue.
- July 6, 1998
  Letter to grantees emphasizing importance of Year 2000 readiness.
- June 15, 1998
  Letter to school business officials.
- May 26, 1998
  Letter to school board presidents.
- April 1998
  Letter reminding customers and service providers to ensure that systems meet the Department's compliance requirements.
- March 1998
  Letter to customers/partners on Year 2000 problem.
- March 1998
  Letter advising all guaranty agencies in the FFEL program of the potential impact of the Y2K problem.
- March 1998
  Letter advising all lenders in the FFEL program of the potential impact of the Y2K problem.
- February 1998
  Letter to all SHEEOs.
- January 1998
  Letter providing background information on Y2K
- January 1998
  Letter to chief financial officers and grantee project directors.
- January 1998
  Letter to reinforce importance of Y2K preparations.
- November 1997
  Letter to address electronic capability requirements.
- October 1997
  Letter informing institutions of deadlines for institutions to use electronic processes and to meet administrative capability requirements.

For additional Y2K resource information see the list of Web site resources included inside this kit.

Questions regarding the Department of Education's Y2K efforts can be directed to:

Elementary and Secondary	**www.y2k@ed.gov**
Postsecondary	**www.ope_y2k@ed.gov**

Frequently Asked Questions
Taken from the Department of Education's Y2K Web Site: www.ed.gov/y2k

What is the Year 2000 problem?

For our purposes, Year 2000 Compliance is defined as: "Year 2000 applications are capable of correct identification, manipulation and calculation using dates, including leap years, outside of the 1900-1999 year range and have been tested as such."

The year 2000 issue, commonly referred to as Y2K, is rooted in the way computer systems have been set up to handle the computation of dates. In many cases, where a date is used in computer code, a two digit field has been used to indicate the year, (i.e., 01/01/98 = January 1, 1998). The system assumes that the first two digits in the year field are "19." With the new millennium approaching, those same systems should reflect 01/01/00 as being "January 1, 2000." However, a non-compliant system will read 01/01/00 as January 1, 1900.

What has the Department of Education done to address the issue?

The Department has established an internal Year 2000 Project Director and Project Coordinators within each of its principal offices. The Department's systems have been categorized in the order of critical functional importance: Mission Critical, Mission Important, and Mission Supportive.

The process of bringing the systems into certifiable compliance has been broken into five phases with milestone completion dates: Awareness - Complete, Assessment - Complete, Renovation - 9/98, Validation - 1/99, and Implementation - 3/99.

What is the Department of Education's date standard format?

CCYYMMDD — 1998/11/23 or 2001/03/12 for example. If subsequent date/time information is transmitted it should follow in descending order of time, i.e., (HH) hour, (MM) minute, and (SS) second.

What if a school's date format is slightly different from ED's standard, e.g., mm/dd/ccyy, instead of ccyy/mm/dd?

All Title IV system's users who participate within TIV WAN will be provided a complete data file layout including the format of date fields. As is currently the case, any data that is transmitted to an application system that does not conform to the provided layout will be rejected by the Title IV system.

What is the Year 2000 requirement for partner institutions' computer hardware?

No special requirements exist for schools' computer hardware, over and above the requirement that those computers maintain and properly transmit data free of Year 2000 anomalies when communicating with ED systems. If a school's PC does not handle dates correctly, resulting in inaccurate data, then the school will be required to repair or replace the equipment so that accurate data will be exchanged.

What is the Year 2000 requirement for partner institutions' computer software?

The same as the requirement for hardware — data must be free from Year 2000 anomalies.

Where do schools get Year 2000 information?

- Your first source should be your computer and systems vendors. To find out if your PC's are compliant we suggest you check with the manufacturer of your computer equipment. You can usually get this information in the manufacturer's website, for example, for PC's manufactured by Dell, the site address is: www.dell.com/, and for Compaq, the site address is www.compaq.com/.
- For more information, visit the Department's website where a tremendous amount of information including "Y2K Best Practices" can be found (www.ed.gov/y2k).

When should my institution complete Year 2000 renovations?

The Department of Education is working diligently to make sure that the systems it uses will continue to function in the year 2000, and we are also working with institutions to be prepared for the year 2000 (Year 2000 Ready). The problems resulting from not being Year 2000 Ready are potentially very serious including data integrity issues and possible interruptions in funding. For that reason the Department is taking every step it can to ensure that all parties concerned will be able to interact with each other in a manner that is consistent with Year 2000 requirements. This means that institutions should, no later than January 1, 1999, have reviewed the Department's technology requirements that were described in the October 1997, Dear Colleague Letter, Gen-97-11, evaluated their current equipment, and where necessary, renovated their computer systems. No later than March 31, 1999, they should have tested those systems for Year 2000 readiness and implemented any necessary renovations.

Currently, all institutions are required to be able to meet the standards of administrative capability outlined in 34 CFR 668.16, and in planning for the future some institutions will have already foreseen and dealt with the Year 2000 problem. For some institutions, upgrading their hardware and software to meet these Year 2000 requirements may present difficulties. If an institution is uncertain about whether it may have problems meeting the Department's Year 2000 guidelines, it should seek whatever help is necessary to address the issue without delay. An institution that is not Year 2000 Ready could jeopardize its ability to draw down Title IV assistance for its students because its data may be flawed due to date errors, or its attempts to electronically communicate with the Department could fail.

Although such an institution may temporarily experience difficulty obtaining electronic information or interrupted access to Title IV funding, the Department will continue to work with the institution to ensure that it overcomes these difficulties. Only if an institution flagrantly ignores its responsibilities to assure Year 2000 compliance will the Department pursue sanctions such as fines or termination against the institution. The Department recognizes how difficult and unique the circumstances are that face institutions working to assure they are Year 2000 Ready, and is much more interested in working with them to achieve a smooth transition to the year 2000 than it is in punishing those who do not.

By the end of 1998, the Office of Student Financial Assistance Programs will promulgate a test schedule, which will provide schools with the opportunity to test the exchange of their data with the Department prior to the Year 2000.

Is the Department of Education-provided software Year 2000 compliant?

The Department's 1999-2000 releases of its Data Provider Software — software which ED issues to institutions for the purpose of providing ED data from those institutions and for communicating with the institutions — will be Year 2000 compliant, and will have been validated and fully tested before issuance. See the individual ED systems write-ups below for details on specific data-provider software applications.

- NSLDS Software (Data Prep)

The National Student Loan Data System (NSLDS) provides data provider software to all organizations required to submit data on a regular basis to NSLDS. The current version of this software already uses four-digit year fields.

A PC-DOS version is available to Guarantee Agencies, Perkins schools, and their servicers. This is being re-written for a 32-bit Windows environment. This new software is scheduled for release in January 1999. The PC-DOS version, which already uses four-digit dates, will be retired in 1999 as schools upgrade their equipment for the new 32-bit version.

NSLDS is implementing additional edits to the software it uses to process data received from data providers to ensure that dates entering the system are not only in four-digit format, but also pass Year 2000 reasonability tests.

- EdExpress

The current version uses a four-digit year but is not yet tested Year 2000 compliant. The next release of the EdExpress scheduled for release in January 1999 will be Year 2000 compliant.

- EdConnect

EdConnect is developed by National Computer Systems (NCS) and GE Information Services (GEIS). NCS develops the user interface, which captures four-digits for the year fields. However, the transmission piece of the EdConnect software developed by GEIS is not Year 2K compliant. GEIS is currently renovating the software to bring this section of the software into compliance. The next release of the EdConnect software, scheduled for release in December 1998 will be Year 2000 compliant.

- Pell Payment Software

The 1998-1999 Pell Payment PC software (both DOS and Windows) is Year 2000 compliant (dates expanded and software functionality changed as needed). The DOS version Pell Payment software was distributed in July 1998 and the Windows version Pell Payment software was distributed in June 1998. The Pell Payment PC software for school years prior to 1998-1999 will NOT be changed or reissued. The volume of data we expect to receive for 1994-1995 through 1997-1998 after 12/31/1999 does not warrant requiring schools or the Department to change their systems/record specifications.

- Campus Based System Software for Fiscal Operations Report and Application to Participate (FISAP)

There will be no DOS version of the FISAP software developed for the 1999-2000 FISAP. The Window version system had passed its Year 2000 stand-alone test in July 1998 and ED distributed the new FISAP in July 1998.

What should a student financial aid administrator ask their systems staff concerning Y2K compliance?

- Is there a Year 2000 plan?
- Get a copy and review it and the dates.
- Make sure that the date formats comply with the Department of Education formats.
- Make sure that implementation of renovated systems is scheduled prior to 3/99.
- Make certain that plan addresses large systems, small databases, PC's, and systems with embedded technology, e.g., fire alarms, phone systems, security systems, medical devices.

What should my institution's systems people be doing about this problem?

They should have a plan that they are working from and have identified the resources necessary to complete it on time.

How can I, a financial aid administrator, confirm the necessary work is being done?

Get frequent updates on the status of the plan. The top management of the school should make this a priority and should get regular updates as well. Once your system is determined to be renovated, conduct a system validation test to verify that it is indeed compliant.

How can I get updated information on the status of the Department of Education's progress in renovating its computer systems?

Every quarter the Department provides a comprehensive report detailing the status of all systems to the Office of Management and Budget. THis report is available on the Education web site: **www.ed.gov/y2k** under the heading "Reports"/

How can I find out the status of Y2K work on other federal agencies' systems?

Each Federal agency has an Internet homepage, some of which provide updated Y2K information. These can all be found by accessing the President's Council on Y2K homepage at: **www.y2k.gov**. Direct links to most of the agencies that Education works with the processing of student aid can be found on the Education Y2K web site: **www.ed.gov/y2k** under the heading "Reports".

This page last modified 10/30/98

Please send questions, comments, and suggestions to y2k@ed.gov or ope_y2k@ed.gov